

Inspector General

United States
Department of Defense



DoD Implementation of Homeland
Security Presidential Directive-12

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 23 JUN 2008		2. REPORT TYPE		3. DATES COVERED 00-00-2008 to 00-00-2008	
4. TITLE AND SUBTITLE DoD Implementation of Homeland Security Presidential Directive-12				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Defense Inspector General, ODIG-AUD, 400 Army Navy Drive, Arlington, VA, 22202-4704				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 90	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/audit/reports> or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE

hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 23, 2008

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND
READINESS
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND
INFORMATION INTEGRATION/DOD CHIEF INFORMATION
OFFICER

SUBJECT: DoD Implementation of Homeland Security Presidential Directive-12
(Report No. D-2008-104)


We are providing this report for your review and comment.

We performed the audit in response to a request from the Office of Management and Budget that the President's Council on Integrity and Efficiency review agency processes and help ensure they are consistent with HSPD-12 and FIPS 201-1. We considered comments from the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer on a draft of the report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Recommendations B.1. and B.2.a. have been clarified in response to management comments. We request additional comments from the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer as detailed in the recommendations table on page ii by July 30, 2008.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AUDROS@dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to Mr. Donald Bloomer at (703) 604-8863 (DSN 664-8863) or Mr. Robert Johnson at (703) 604-9024 (DSN 664-9024). The team members are listed inside the back cover.


Paul J. Granetto
Principal Assistant Inspector General
for Auditing



Results in Brief: DoD Implementation of Homeland Security Presidential Directive-12

What We Did

We performed the audit in response to a request from the Office of Management and Budget that the President's Council on Integrity and Efficiency review agency processes and help ensure they are consistent with HSPD-12 and FIPS 201-1. We evaluated DoD business processes to determine whether they comply with directives and standards to develop secure and reliable Personal Identity Verification (PIV) credentials.

What We Found

DoD is not complying with HSPD-12 requirements, has not issued comprehensive HSPD-12 implementation guidance to DoD Components, and has not met HSPD-12 implementation milestones. DoD policy on physical access controls needs to be updated to comply with HSPD-12 policy objectives. Specific examples follow.

- DoD did not meet Government-wide milestones for completing background checks.
- Personnel at stations that issue the Common Access Card cannot electronically verify whether card applicants have initiated or completed a National Agency Check with Written Inquiries.
- DoD displays the full Social Security number on the Geneva Conventions credential, increasing the risk of identity theft.
- Components are purchasing equipment that is not compliant with HSPD-12.
- DoD is using barcode technology on the Defense Biometric Identification System credential that is not equivalent to mandatory HSPD-12 security features.
- DoD's current PIV credential does not meet interoperability requirements and needs to be updated.

What We Recommend

- Issue comprehensive DoD HSPD-12 implementation guidance within 90 days.
- Revise and update DoD Directives and Instructions to incorporate Federal Information Processing Standards requirements.
- Submit proposed end-state PIV credential to GSA for conformance testing.

Client Comments and Our Responses

The Under Secretary of Defense (Personnel and Readiness) agreed with two, partially agreed with two, and deferred on three recommendations. He has agreed to work with other DoD offices in the next 3 months to identify milestones to incorporate in the DoD HSPD-12 Implementation Plan. The Under Secretary of Defense (Intelligence) agreed with three, partially agreed with two, and disagreed with two recommendations. He required all new access control systems to comply with FIPS 201-1. The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer disagreed with developing a FIPS 201-1-compliant authentication certificate within 6 months, citing extenuating circumstances. In the absence of obtaining a waiver, DoD should comply with FIPS 201-1. We revised two recommendations to clarify their intent. We request comments on the final report by July 30, 2008. Please see the recommendations table on the back of this page for details.

Recommendations Table

Client	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Personnel and Readiness	A.1.b., B.1., B.2.a.,	A.1.a., A.1.c., A.2., B.2.b.
Under Secretary of Defense for Intelligence	A.2., B.2.a., B.3.a.1., B.3.a.2.,	B.2.b., B.3.a.3., B.3.b.
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer	A.3.	

Please provide comments by July 30, 2008.

Table of Contents

Results in Brief	i
Introduction	1
Objectives	1
Background	1
Review of Internal Controls	2
Finding A. Implementation of Directive	3
Recommendations	9
Finding B. Issuance of Implementation Guidance	15
Recommendations	20
Appendices	
A. Scope and Methodology	25
Prior Coverage	26
B. Guidance on Identification and Access Control	27
C. Client Comments on the Findings and Audit Response	32
D. Glossary	53
E. List of Acronyms and Abbreviations	55
Client Comments	
Under Secretary of Defense for Personnel and Readiness	57
Under Secretary of Defense for Intelligence	67
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer	73

Introduction

Objectives

Our overall audit objective was to determine whether DoD is complying with the requirements of Homeland Security Presidential Directive-12 to enhance the quality and security of the identification that Federal employees and contractors use, and to implement common personal identity verification (PIV) credentials¹ that will be strongly resistant to terrorist exploitation. Specifically, we evaluated whether DoD business processes comply with directives and standards to develop PIV credentials that are secure and reliable forms for identifying DoD employees and contractors.

Background

President Bush signed the Homeland Security Presidential Directive-12 (HSPD-12) on August 27, 2004. HSPD-12 objectives are to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 establishes a mandatory, Government-wide standard for secure and reliable forms of identification issued by Federal agencies to their employees and contractors. The Presidential Directive defines secure and reliable identification as being (a) issued based on sound criteria for verifying an individual employee's identity; (b) strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) capable of rapid electronic authentication; and (d) issued only by accredited providers. As required by HSPD-12, the Secretary of Commerce promulgated Federal Information Processing Standard (FIPS) 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors," February 25, 2005, which established minimum requirements for a Federal personal identity verification system (PIV-I) and detailed technical specifications of components and processes required for interoperability of PIV cards (PIV-II). On March 2006, the Secretary of Commerce issued FIPS 201 Change Notice 1 (FIPS 201-1), updating the requirements established by FIPS 201.

Office of Management and Budget (OMB) Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive-12 Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005, establishes timelines and milestones for FIPS 201-1-compliance. OMB Memorandum M-07-06, "Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials," January 11, 2007, required all Federal agencies to submit their FIPS 201-1-compliant credential to the General Services Administration for testing by January 19, 2007. The memorandum announced that agencies would be contacted by their Inspector General to ensure business processes are being followed to foster the environment of trust needed for the credentials to be accepted by departments and agencies when deemed appropriate in implementing HSPD-12.

¹ See Appendix D for definitions of "credentials" and other terms used in this report.

Agencies may elect to implement HSPD-12 through either a transitional or an end-point credential. DoD is the only agency granted transitional status by OMB because DoD already has a smart card program. DoD must achieve the end-point credential specification for all cardholders at some point. OMB established October 27, 2006, as the date for issuing an initial end-point credential by all agencies; however, OMB has not established a deadline for DoD to achieve initial operational capability. In early 2007, DoD began to issue a limited number of transitional credentials to individuals whose previous credentials had expired. In the quarterly DoD PIV Status Report dated December 26, 2007, DoD reported it had issued 56 credentials as of March 2007. After the issuance of our draft report, the April 1, 2008, quarterly DoD PIV Status Report cited 108,778 total PIV cards issued: 83,659 to employees and 25,119 to contractors. DoD had not completed development of an end-point credential as of May 2008.

The Under Secretary of Defense for Personnel and Readiness is responsible for the timely implementation of HSPD-12 for the Department of Defense. The Defense Manpower Data Center (DMDC) has been assigned responsibility for development of a DoD common access card meeting the requirements of HSPD-12. We visited the DMDC East facility to determine the stage of HSPD-12 compliance and to review common access card (CAC) testing, issuance, and infrastructure. To determine HSPD-12 compliance at installations, we also visited 13 military and Coast Guard installations—all with CAC issuance facilities. We visited Defense Supply Center-Philadelphia and the Defense Logistics Agency concerning a photoless ID cardholder.

Review of Internal Controls

We identified an internal control weakness for DoD as defined by DoD Instruction 5010.40, “Managers’ Internal Control (MIC) Program Procedures,” January 4, 2006. DoD did not have adequate internal controls to ensure DoD compliance with the requirements of HSPD-12. DoD has not issued comprehensive HSPD-12 implementation guidance. Further, existing guidance pertaining to various aspects of HSPD-12 implementation, such as DoD Regulation 5200.08-R and DoD Directive 1000.25, is contrary to HSPD-12 policy. See finding B for specific results of those weaknesses. Implementing the recommendations made in this report will correct the weaknesses. A copy of this report will be provided to the senior official responsible for internal controls in DoD.

A. Implementation of Directive

DoD did not meet the milestones approved by the Office of Management and Budget (OMB) in 2005 for compliance with Homeland Security Presidential Directive-12 (HSPD-12) by 2010. DoD missed these milestones in part because it declared a “strategic pause” in HSPD-12 implementation from April to December 2007, and has not met HSPD-12 minimum standards for its transitional program. In addition, DoD has not provided centralized funding for critical required elements of HSPD-12 implementation. As a consequence, the intended benefits of HSPD-12 to enhance security, increase Government efficiency, reduce identity fraud, protect personal privacy, and reduce the potential for terrorist exploitation will not begin to be realized by the Department until at least 2012.

Implementation Milestones and Strategic Pause

In June 2005 DoD submitted its HSPD-12 Implementation Plan to OMB for approval. OMB approved DoD milestones for the Personal Identity Verification (PIV)-I and PIV-II requirements to support DoD achieving full compliance with HSPD-12 requirements by April 2010. DoD’s updated January 2008 HSPD-12 Implementation Plan documents the failure of the Department to meet critical HSPD-12 implementation milestones. Implementation challenges remain that threaten to further delay full compliance with HSPD-12 requirements.

DoD attributes the adjustments in implementing HSPD-12 milestones to a strategic pause taken to update infrastructure for issuing CACs. DoD’s transition to a Web services architecture has not been as trouble-free as anticipated. In April 2007, DoD declared a strategic pause in the implementation of the Web version of its issuance infrastructure until December of 2007. After the strategic pause, DoD recommenced with the upgrade of its issuance infrastructure to the Web service architecture and full compliance with the FIPS 201-1, PIV-II requirements. DoD will need a year from the December 2007 reinitiation to upgrade the entire infrastructure. The strategic pause directly affected the Department’s ability to achieve full implementation of HSPD-12 PIV-I and PIV-II requirements.

Personal Identity Verification-I Requirements

PIV-I requirements are the minimum requirements for a Federal personal identification verification system that meets the control and security objectives of HSPD-12, including personal identity proofing and registration, issuance, and privacy protection.

1. PIV identity proofing and registration requirements include the initiation of a National Agency Check with Written Inquiries (NACI) background check. FIPS 201-1 Part 2 requires that when a PIV credential is issued to a Federal employee or contractor without a completed NACI background check, the credential must be electronically distinguishable from that issued to an individual who has completed a NACI background check.

2. PIV issuance requirements state that, at the time of issuance, the PIV applicant's identity must be verified as the person intended to receive the PIV credential and for whom the background check was completed.
3. Protecting personal privacy is a requirement of the PIV system.

Background Checks

FIPS 201-1 requires that employees and contractors who are issued a PIV credential undergo, at a minimum, a NACI or OPM or National Security community investigation equivalent background check. The background check must be initiated and the fingerprint check completed before the issuance of any PIV credential. Further, at the time of PIV issuance, the issuing official is required to verify the status of the NACI process for the applicant (completed or ongoing). Credentials issued to individuals without a completed NACI or the equivalent must be electronically distinguishable from credentials issued to individuals who have a completed investigation.

Automated Verification of Status

The Director of DMDC issued a memorandum on September 12, 2007, stating that DMDC is working closely with the Office of the Deputy Under Secretary of Defense for Intelligence, Counterintelligence, and Security to establish an automated capability to verify the status of an individual's background check. However, DoD does not intend to produce identity credentials that will include an electronic indication of the status of a NACI. Further, DoD has yet to establish an automated mechanism to verify that all individuals receiving the PIV credential have at least initiated, if not completed, the required NACI background investigation.

Deadlines for Completion of Background Checks

Office of Management and Budget Memorandum M-05-24 mandates that agencies:

- by October 27, 2007, verify or complete background checks for all current employees and contractors, except for agency employees employed more than 15 years; and
- by October 27, 2008, complete background checks for all Federal department or agency employees employed more than 15 years.

DoD did not meet the OMB deadline of October 27, 2007, for current employees and contractors. According to DoD's January 2008 Implementation Plan, as of December 26, 2007, the following numbers of DoD employees and contractors had not completed the required background checks.

DoD Employees and Contractors With Incomplete Background Checks

Military or Civilian	1,240,214
Contractors	196,185
Total	*1,436,399

*DoD's January 2008 Implementation Plan noted that these numbers may not be an accurate reflection of the completed qualifying investigations, but a reflection of data quality in the DoD Joint Personnel Adjudication System.

Privacy Requirements

HSPD-12 explicitly states that protecting personal privacy is a requirement of the PIV-I implementation policy. All departments and agencies shall implement the PIV system in accordance with the spirit and letter of privacy controls specified by HSPD-12 and in Federal privacy laws and policies. The DoD Geneva Conventions credential for members of the uniformed services does not comply with HSPD-12 or with Federal policies and requirements to reduce identity fraud and protect personal privacy.

The continued display of Social Security numbers on the DoD Geneva Conventions credential is the result of adherence to guidance that does not reflect changes in Federal policies, technological advancements, or the increased need to protect personal information. DoD began displaying the Social Security number on identification badges in 1967. In 2007 OMB instructed Federal departments and agencies to take steps to reduce the risk related to loss of personally identifiable information. In 2007 OMB issued guidance to Federal agencies to eliminate unnecessary use of Social Security numbers and strengthen protection of personal information from loss or theft. In 2006 Congress identified the inherent risk of displaying the full Social Security number on identification credentials and the need to protect individuals' right to privacy and reduce the risk of identity theft. Printing of the Social Security numbers in conjunction with the individuals' dates of birth on DoD credentials unnecessarily exposes individuals' personal privacy information and increases the risk of identity theft.

In response to an FY 2007 congressional request, DoD issued a report to Congress, "Omission of the SSN from the Department of Defense Military Identification Cards," May 23, 2007. In it, the Under Secretary of Defense for Personnel and Readiness (USD [P&R]) recommended removing the full Social Security number from view on identification credentials, instead displaying only the last four digits. The full Social Security number would be retained in the portable data file 417 two-dimensional barcode and the integrated circuit chip on the credential. No timetable was provided to implement the recommendation, however, nor did the report specify who was responsible for implementation. The current appearance of DoD's Geneva Conventions credential unnecessarily compromises personal privacy and increases the risk of identity theft and the potential for terrorist exploitation. DoD should immediately require USD(P&R) to implement the recommendation to print only the last four digits of the Social Security number on the Geneva Conventions credential.

Personal Identity Verification-II Requirements

PIV-II requirements are the detailed technical specifications of components and processes required for interoperability of PIV credentials for personal authentication, access controls, and PIV card management across Federal departments and agencies. HSPD-12 envisions that when Federal departments and agencies issue and manage the required, fully interoperable PIV credentials, individuals' identity can be authenticated Government-wide, thus increasing the security of Federal facilities and information systems. DoD did not meet the March 2006 PIV-II initial operational capability implementation milestone approved by OMB in the DoD Implementation Plan, nor did DoD meet the October 2006 OMB milestone for PIV-II implementation.

DoD PIV PKI Authentication Certificate

One of the technical specifications for a PIV-II-compliant card is a Public Key Infrastructure (PKI) authentication certificate. Because of the Department's strategic pause, resources allocated to support the development of the authentication certificate were reallocated. The reallocation has caused a delay in the development, testing, and issuance of the authentication certificate. As a result, DoD now plans to delay issuance of the authentication certificate until the third quarter of FY 2008. The current DoD credential contains three certificates: (1) digital signature certificate, (2) key management certificate, and (3) card authentication certificate. The DoD Public Key Infrastructure Program Management Office (PKI PMO), tasked with developing the required PIV PKI authentication certificate, chose to develop a new, fourth certificate to meet HSPD-12, FIPS 201-1, and PIV PKI authentication requirements rather than modify an existing certificate.

The PKI PMO elected to develop authentication certificates using the Federal bridge policy, despite the HSPD-12 requirement that became effective January 1, 2008, to use Common Policy object identifiers. DoD has been lobbying since 2006 to have changes made to FIPS 201-1 so that the Federal bridge policy would be adopted for DoD's PIV PKI authentication certificate, rather than working toward meeting the current FIPS 201-1 Common Policy requirements. The PKI PMO program manager stated that DoD's unique infrastructure is too robust to use the Common Policy object identifiers. DoD is not currently planning to use Common Policy object identifiers in certificates unless the National Institute of Standards and Technology (NIST) promulgates two modifications to the Federal Common Policy object identifiers. The requested modifications to the Common Policy are as follows.

- **Increase the frequency of issuance of the certificate revocation list (CRL).** DoD issues the CRL once every 24 hours from 14 certificate authorities. The Common Policy's smaller 18-hour window will place a strain on system performance, according to DoD.

- **Shorten the NextUpdate time in the CRL.** DoD NextUpdate time is 7 days, whereas the Common Policy time is no longer than 48 hours. According to DoD, reduction in the number of days for the next update would cause a large increase in CRL traffic and potentially consume network bandwidth well above what the DoD network is meant to accommodate.

DoD plans to use Common Policy object identifiers in the PIV PKI authentication certificate only after FIPS 201-1 is revised to meet DoD objections, and estimates that implementation will take 1 year. The petition for the two changes has been submitted to the Federal PKI policy authority for approval, but no date has been established for consideration of the two modifications.

DoD PIV End-Point Applet

Because DoD has elected to maintain its current CAC infrastructure, DoD must develop a PIV end-point applet to achieve full interoperability with other Federal agencies for the DoD PIV credential, as required by HSPD-12. The PIV applet, developed by DMDC, will be the intermediary that should allow readers compliant with HSPD-12 to access the necessary information on the DoD credential. After the required approval of the DoD PIV applet by NIST, General Services Administration (GSA) testing of the PIV credential with all the required components must be successfully completed before the DoD credential can be considered end-point-PIV-compliant.

DoD Transitional Credential

OMB granted DoD transitional status for implementation of the PIV system in June 2005. DoD was given until April 2010 for its PIV system to achieve full operational capability for its approximately 3.5 million PIV credentials. DoD plans to issue PIV credentials to DoD employees and contractors as their CACs expire. DoD CACs expire 3 years after issuance. DoD has started issuing some DoD PIV transitional credentials as card issuance workstations are updated to produce the transitional credentials.

Not all cardholders whose CACs expire receive the DoD transitional credential because not all card issuance workstations can issue the transitional credential. Some issuance sites are instructed to exhaust their current stock of noncompliant cards before issuing the DoD PIV transitional credential.

The DoD PIV transitional credentials do not contain either the required PIV PKI authentication certificate or the DoD PIV applet. According to DoD, the transitional credential can be updated at some future time with an approved and tested PIV PKI authentication certificate and PIV applet through downloads from the DMDC Web portal. DoD now projects PIV system full operational capability will occur in the summer of 2012. Achieving full operational capability remains problematic for DoD because of unresolved infrastructure issues and the unavailability of updated workstations required to issue the DoD transitional and eventually the fully compliant end-point PIV credentials.

DMDC is responsible for updating the centrally funded Real-time Automated Personnel Identification System (RAPIDS) workstations to RAPIDS version 7.2 to produce DoD PIV credentials for DoD installations in the continental United States by December 12, 2008. No schedule for deployment of updated RAPIDS workstations has been announced for four installations outside the continental United States, including two in Germany and one each in Djibouti and Greenland. No central funding is planned at installations for acquisition of equipment needed for the transition to physical access control systems that are compliant with HSPD-12 and FIPS 201-1. Installation commanders are responsible for granting access privileges and for funding to update or replace physical access control systems to bring them into compliance. The Military Services did not provide any plans, milestones, or dedicated resources to update or replace physical access control systems to comply with HSPD-12 and FIPS 201-1 requirements.

Conclusion

Inconsistent agency approaches to security of facilities and information systems are inefficient and costly, and they increase risk to the Federal Government. On August 27, 2004, President Bush issued a directive to Federal agencies to implement a Government-wide standard for secure and reliable forms of identification for Government employees and contractors. Successful implementation was expected to increase the security of Federal facilities and information systems. The President directed Federal agencies to promptly implement the mandatory, Government-wide standard for secure and reliable forms of identification.

DoD has not met key HSPD-12 implementation milestones for completion of background checks, verification of completed or initiated background checks, or Government-wide interoperability. Additionally, DoD must modify its current Geneva Conventions PIV credential to reduce the potential for identity fraud. Unresolved DoD CAC infrastructure problems continue with no firm date for resolution. As a consequence, the intended benefits of HSPD-12 to enhance security, increase Government efficiency, reduce identity fraud, protect personal privacy, and reduce the potential for terrorist exploitation will not begin to be fully realized by the Department until 2012 or later.

Client Comments on the Finding and Audit Response

Please see Appendix C for complete client comments and audit responses on the finding.

Recommendations, Client Comments, and Audit Response

A.1. We recommend that the Under Secretary of Defense for Personnel and Readiness:

a. Submit DoD's proposed personal identity verification end-point credential to the General Services Administration for conformance testing and approval within 1 month of completion of Recommendation A.3.

Client Comments. "OUSD (P&R) concurs with this recommendation. OUSD (P&R) will submit its Common Access Card (CAC) Personal Identity Verification (PIV) end-state credential to the General Services Administration (GSA) for conformance/ interoperability testing within one month of completion of recommendation A3 (expected by the end of 2008). OUSD (P&R) fully expects the card to pass all areas DoD has agreed to support in accordance with the January 2008 DoD HSPD-12 Implementation Plan."

Audit Response. Client comments are responsive.

b. Test the General Services Administration-approved personal identity verification credential for compatibility with DoD systems before making it available to DoD employees and contractors.

Client Comments. "OUSD (P&R) partially concurs with this recommendation. As outlined in the above response, DoD will conduct GSA conformance testing by the end of calendar year 2008. However, OUSD (P&R) non-concurs with completing GSA testing before making the credential available to DoD employees and contractors. DoD was approved by OMB as a legacy card issuer and, as such, is authorized to implement transitional credentials that can be updated in the future to conform to FIPS 201 specifications. This provides significant benefit with minimal adverse impact to the operational community. Additionally, DoD has an established testing process with the Military Services and DoD Components that is monitored by the DoD's Identity Protection Senior Coordinating Group (IPMSCG). Prior to being moved to our operational CAC inventory, all emerging CAC platforms (including DoD's CAC PIV transitional and end-state configurations) are evaluated and approved for release by the IPMSCG's Test and Evaluation Work Group (TEWG). This group consists of representatives from Military Service CAC-PKI labs and several DoD Components."

Audit Response. Client comments are not responsive. OMB Memorandum M-07-06, "Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials," January 11, 2007, requires all agencies to provide to GSA an end-point credential with their agency's standard configuration for testing. If GSA finds configuration problems, the agencies are required to submit their standard configuration for retesting once the required corrections are made. The OMB memorandum also states

that agencies should consider not issuing new credentials until all problems identified in testing are resolved. A credential that has passed GSA testing may not necessarily be compatible with all DoD systems. Therefore, it would be counterproductive to issue credentials that impede DoD operations. OMB required all agencies to begin issuing compliant credentials by October 27, 2006, either through the services of GSA and the Department of Interior or by performing this function internally. DoD's internal transitional program is not exempt from this requirement. Transitional status does allow DoD additional time to obtain full operational capability because of the large volume of compliant credentials to be issued. We request that the USD(P&R) reconsider his position on the recommendation and provide additional comments on the final report.

c. Implement within 2 months the recommendation in DoD's Report to Congress, "Omission of the SSN from the Department of Defense Military Identification Cards," May 23, 2007, to display only the last four digits of the Social Security number on the Geneva Conventions credential, while migrating toward completely eliminating the display of the Social Security number on all identification credentials.

Client Comments. "OUSD (P&R) partially concurs with this recommendation. We note that the implementation of DoD's Report to Congress, 'Omission of the SSN from the Department of Defense Military Identification Cards,' May 23, 2007 is not a requirement of HSPD-12, associated NIST standards, or relevant OMB HSPD-12 guidance.

The Department is executing the policy, procedural and technical steps required to remove the SSN from DoD ID cards. The truncation of the visible SSN on Geneva Conventions credential to four-digits is one step in the plan recommended to Congress. However, this step will take place in a coordinated fashion as the feature is made available within the issuance software (e.g., RAPIDS) and existing credentials are replaced after the update is completed. We expect to begin implementing this change during calendar year 2008."

Audit Response. Client comments are responsive. We recognize the actions set forth in the Report to Congress to truncate the Social Security number on the Geneva Conventions credential to the last four digits.

A2. We recommend that the Under Secretary of Defense for Personnel and Readiness, in conjunction with the Under Secretary of Defense for Intelligence, centrally fund the acquisition and installation of HSPD-12-compliant access control equipment throughout the Department and establish Component-specific milestones for both acquisition and installation of the equipment.

Client Comments (OUSD [P&R]). "OUSD (P&R) defers on a response to this recommendation; the responsibility for centrally funding the acquisition and installation of access control equipment does not fall under the purview of OUSD (P&R). Responsibility for force protection and physical security standards falls under the purview of the Office of the Under Secretary of Defense for Intelligence (OUSD (I))."

Audit Response. The client deferred to the OUSD (I) for comments on this recommendation.

Client Comments (OUSD [I]). “OUSD (I) nonconcurs with the recommendation as currently stated. OUSD (P&R) has the responsibility for fielding a FIPS 201 compliant identification credential to Federal Employees and Contractors only, which is expected to be complete by the end of FY 2012. OUSD (P&R) does not have Research, Development, Test and Evaluation (RDT&E), acquisition or oversight authority for access control equipment.

We do not support a central acquisition approach for access control equipment at present, as we are not staffed to support oversight of an effort of this magnitude, nor is the Air Force, who is the lead for Research, Development, Test and Evaluation for access control physical security equipment. See references DoDI [Instruction] 5143.01, Under Secretary of Defense for Intelligence (USD (I)), Nov 2, 2005 and DoDI 3224.3 Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E), Oct 1, 2007.)

Central acquisition will be problematic for all components, as there are other issues that would significantly impact this approach. These issues include: Congress provided no funding to implement this mandate and therefore any centralized acquisition would require reductions in other Physical Security and Department procurement requirements; HSPD-12 does not apply to National Security Systems and Special Risk Security Provisions; ability to adapt existing legacy systems to meet HSPD12; and the install of access control equipment must be in concert with military design and construction projects for access control points.

OUSD (I) concurs that any new acquisition and installation of access control equipment throughout the Department must conform to the mandates of HSPD-12 and associated OMB policy for interoperability. This stipulation has been included in formally staffed draft policy, Directive Type Memorandum 08-004, Policy Guidance for DoD Access Control, which is pending USD (I) signature as of this submission.”

Audit Response. Client comments are partially responsive. We agree with the client that any new acquisition and installation of access control equipment throughout the Department must conform to the mandates of HSPD-12 and associated OMB policy for interoperability. HSPD-12-compliant access control equipment will allow secure and rapid electronic verification of a credential holder’s identity.

Electronic authentication of identities is essential to realizing the full security benefits of HSPD-12 requirements. The procurement and installation of HSPD-12-compliant access control systems is crucial to meeting this requirement. On April 9, 2008, the congressional Subcommittee on Government Management, Organization, and Procurement held a hearing on “Federal Security: ID Cards and Background Checks.” HSPD-12 was the major topic of discussion.

At the hearing, the Government Accountability Office (GAO) reported that most agencies were not using the electronic authentication on the PIV credentials and had not developed an implementation plan for these capabilities. One reason for this, according to GAO, is that agencies anticipate having to make substantial financial investments to fully implement HSPD-12. Committee members were greatly disturbed to learn of the practice of using the HSPD-12-mandated PIV credentials as flash passes. Members called the practice a waste of resources and asked whether additional funding is required for full implementation and use of the HSPD-12 credential. The full realization of the HSPD-12 goal to enhance the protection of DoD installations and facilities resources should be a DoD priority.

We request that the USD(I) reconsider his position and provide additional comments regarding the most appropriate mechanism to fund acquisition and installation of the PIV-compliant access control equipment throughout DoD.

A.3. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer develop the mandatory Public Key Infrastructure authentication certificate that complies with FIPS 201-1 requirements to use Common Policy object identifiers for cross-agency verification of cardholders' identification within 6 months.

Client Comments. “Recommend that the DODIG remove the recommendation A.3 from the final report based on the extenuating and mitigating circumstances surrounding this FIPS 201 requirement. DoD PKI PMO has endeavored, in good faith, to comply with all FIPS 201 requirements. Current plans, as stated in the January 2008 update to the DoD HSPD-12 Implementation Plan [JANDODPLAN], indicate that the PIV_Auth certificate will be instantiated on the DoD PIV credential as soon as technically possible. Lack of compliance with the Common Policy OIDs [object identifiers] does not affect the interoperable use (cross-agency verification of cardholder's identity) of the CAC with either DoD or other Federal Agency physical or logical systems.

Comment: Disagree with this recommendation A.3. The recommendation does not recognize or consider the extensive mitigating or extenuating circumstances explained in the January 2008 update to DoD HSPD-12 Implementation Plan [JANDODPLAN] nor does it show consideration of the reported work accomplished by the DoD PKI PMO to comply with the FIPS 201 requirement for instantiation of a PIV Authentication certificate (PIV_AUTH). The DoD PKI PMO has planned for the deployment and is testing the issuance of a PIV_AUTH certificate and has estimated beginning the issuance of this certificate on the DoD PIV credential in 3QFY08 [JANDODPLAN]. Those plans are aligned with but contingent on fielding of another version of the RAPIDS issuance software. The DODIG recommendation does not consider the lack of adequate memory available on the current CAC crypto module, the availability of the cryptomodules with the necessary storage capacity, necessity for performance testing on issuance and use or examination of the operational impacts of using RSA [Rivest, Shamir, and Adleman] 2048 end entity certificates. The DODIG recommendation does not consider that the DoD PKI PMO has reported, for several years, to OMB and the Federal PKI Policy

Authority (FPKI PA), the risks of changing DoD PKI CA operations to conform to the specified Federal Common Policy requirements. DoD PKI PMO has been endeavoring to work with the FPKI PA to make mutually acceptable changes to the Federal Common Policy Certificate Policy (CP). The DODIG recommendation does not recognize or consider in extenuation that the DoD PKI PMO has been very proactive about informing the FPKI PA and NIST about the operational challenges full compliance with FIPS 201 represents to DoD.”

Audit Response. Client comments are not responsive. We recognize there are complexities involved in fielding the FIPS 201-1-compliant credential. Although the client states that the current CAC does not accommodate the memory available on the current CAC crypto module, there are cards available that will accommodate memory requirements. Further, NIST officials have stated that for interoperability it is important that the PIV Authentication Key asserts the PKI Common Policy object identifiers. We request that the ASD(NII)/CIO provide additional comments on how he will meet FIPS 201-1 requirements.

B. Issuance of Implementation Guidance

DoD Components are attempting to address security and personnel identification concerns in an ad hoc manner. Formulation and issuance of HSPD-12 implementation guidance were not priorities for DoD because senior management chose to establish and implement less stringent access control requirements rather than HSPD-12 PIV-I standards. DoD will not realize increased security and efficiencies until DoD Components are provided with comprehensive HSPD-12 implementation guidance mandating the issuance of secure and reliable credentials and the use of updated, compliant access control systems at DoD installations.

DoD Component Implementation Efforts

HSPD-12 requires that access to Federal facilities or information systems be granted to Federal employees and contractors based on secure and reliable forms of identification that meet the Federal standard established by the Secretary of Commerce. FIPS 201-1 contains the minimum standards that agencies are to implement to comply with HSPD-12 requirements. DoD has not issued comprehensive implementation guidance that incorporates the minimum standards, leaving DoD Components without specific guidance to address HSPD-12 requirements for security and personnel identification.

Without official guidance, Components have improvised. For instance, background checks vary by Component; Components have purchased noncompliant HSPD-12 equipment; a DoD installation has issued a photoless identification credential; and Components have been authorized to issue Defense Biometric Identification System (DBIDS) credentials instead of PIV credentials.

Background Checks

DoD Components have not met NACI background check requirements. Because of the large number of Army personnel requiring NACIs and the associated cost, the Army is considering requesting a waiver of the immediate HSPD-12 mandated NACI background checks until the members' current CAC cards expire or individual are due for periodic reinvestigations. USD(P&R) issued a memo on March 9, 2007, expanding CAC eligibility to include foreign national partners who have been properly vetted and who require access to DoD facilities or information systems. This memo establishes the vetting requirement when an international security agreement is in place. However, the guidance does not address a vetting process for foreign nationals requiring a CAC for access to DoD installations and information systems in countries where no international security agreement has been established, such as Afghanistan and Iraq. One Air Force base does not require contractors that have only physical access to the installation to receive background checks unless the contractors are first line supervisors. One Defense agency required contractors receiving a CAC to undergo only a NAC. During our review, a Defense Agency Chief of Personnel Security issued an agency-wide e-mail on

June 19, 2007, requiring contractors receiving a CAC to undergo a NACI background check.

Equipment Purchases

One Army installation purchased several card readers without ensuring they complied with HSPD-12. An Air Force installation was in the process of purchasing equipment that was not on the GSA Approved Products List as required by OMB; however, when made aware of this, officials at the Air Force installation stopped procurement to ensure they purchased only products that were on the GSA Approved Products List.

Photoless Identification

On February 4, 1999, the Commanding Officer at the Naval Support Station (now Naval Support Activity) in Philadelphia, Pennsylvania, issued a waiver for a photo identification badge to a Defense Logistics Agency (DLA) employee working at Defense Supply Center-Philadelphia (DSCP) who objected for religious reasons to having his photograph taken and displayed on the identification badge. Guidance is required on evaluating the legitimacy of requests that deviate from established access control policy.

DBIDS Credentials

DoD has authorized Components to issue a DBIDS card to employees and contractors who require only routine (180 days or greater) physical access. This practice deviates from HSPD-12.

DoD HSPD-12 Policy and Guidance

Formulation and issuance of HSPD-12 implementation guidance were not priorities for DoD senior management. DoD Components' problems with implementation can be attributed to the lack of comprehensive guidance. After issuing proposed HSPD-12 implementation policy for coordination in April 2006 and not reaching consensus among DoD Components, DoD established a working group to develop comprehensive guidance for implementation of HSPD-12, but the group has made only limited progress. Meanwhile, DoD senior management chose to establish and implement less stringent access control requirements rather than those established by HSPD-12.

Formulation of Policy

On April 24, 2006, the Defense Human Resource Agency (DHRA) sent out a request for coordination on proposed HSPD-12 implementation policy. DHRA, the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD [NII]/CIO), the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD [AT&L]), DMDC, and USD(I) could not agree on the proposed HSPD-12 implementation policy. As a result, implementation languished until August 27, 2007, when the USD(I) Physical Security Directorate requested an HSPD-12 Strategy Working Group meeting with DHRA, ASD (NII/CIO), USD (AT&L), and DMDC group members to complete implementation guidance. As of March 2008, DoD had not issued DoD HSPD-12 implementation guidance other than updates to DoD Regulation 5200.08-R for physical access security.

Issuance of Guidance

DoD Regulation 5200.08-R does not address specific background check requirements or equipment purchases from the GSA Approved Products List. Furthermore, it is inconsistent with HSPD-12 because it allows DBIDS and other forms of identification that are not compliant with FIPS 201-1.

NACI Requirement

DoD Regulation 5200.08-R states that “A National Agency Check with Inquiries or equivalent national security clearance National Agency Check with Local Agency Checks including Credit Check is required for permanent issuance of the credential.” This statement leaves open such questions as which DoD entity should pay for the background checks for contractors and what kind of background check is required for foreign nationals.

Approved Products List

To ensure Government-wide interoperability, DoD must acquire products and services that are compliant with FIPS 201-1 and included on the GSA Approved Products List as required by OMB. In some instances, DoD Components have acquired products that are not on the GSA Approved Products List. DoD has not issued any guidance to the Components requiring use of the Approved Products List.

DBIDS Credential and Physical Access Control Systems

OMB instructed agencies to be careful not to develop policies that contradict HSPD-12 standards for identity proofing and issuance of credentials. HSPD-12 standards mandate that all Federal employees and contractors requiring routine access for 180 days or longer receive a PIV-compliant credential and undergo a NACI or equivalent background check. DoD Regulation 5200.08-R authorizes personnel requiring only routine physical access to receive a DBIDS credential and undergo the less rigorous NAC. Granting routine access to DoD installations to personnel who have only a NAC background check does not fully comply with the HSPD-12 policy objective to enhance security and protect physical and human capital assets on DoD installations.

According to DoD Directive 1000.25, DBIDS is a fully configurable force protection system and serves as a physical access control and critical property registration system. Yet the system does not meet the minimum standards of FIPS 201-1 to verify the claimed identity of individuals seeking physical access to Federal Government facilities. DoD Components are required to purchase and maintain this physical access control system through DMDC. However, DBIDS uses card readers and scanners that are not on the GSA Approved Products List as required by OMB.

Neither the DBIDS system nor the card is configured to operate with HSPD-12 security features such as PKI certificates, the Card Holder Unique Identifier, and biometrics embedded in the integrated circuit chip of the credential. Further, the use of barcode technology on the DBIDS credential does not enhance security because the barcode, a static physical card feature, cannot deter fraud, prevent counterfeiting, or protect personal privacy. According to comments from the Smart Card Alliance on a report by the

Department of Homeland Security, DHS-2006-0030, May 7, 2007, barcode technology is not secure and not adequate to meet Federal security and privacy requirements. DBIDS does not meet the FIPS 201-1 minimum standards to enhance security, increase Government efficiency, and protect personal privacy.

Of the 16 installations we visited in the continental United States, 6 formerly used or continued to use DBIDS as their physical access control system for individuals requiring only physical access. Four of the six installations used barcode technology, without biometrics, to authenticate the identity of the credential holder before granting access to the installation. The fifth, an Army installation, discontinued the use of DBIDS because the maintenance of the system was too expensive and the system did not perform as required. The sixth, an Army installation, used the DBIDS access control system but not the DBIDS card, which is not compliant with HSPD-12 standards.

Additionally, officials at one of the four installations, a Navy installation, stated that their DBIDS equipment is deteriorating and that they did not have the funds to maintain it. Instead of scanning the DBIDS credential, they use it as a flash pass.

Photo Identification Requirements

FIPS 201-1 requires that PIV credentials be issued only to individuals whose identity has been verified and whose background investigation is either on record or initiated. Identity verification for the PIV credential requires two forms of identity, including at least one valid State or Federal Government picture identification. The PIV credential requires a photograph showing the full frontal pose from top of the head to shoulder and placed in the upper left corner of the credential. Waivers to FIPS 201-1 are not allowed.

On February 4, 1999, the Commanding Officer at the Naval Support Station (now Naval Support Activity) in Philadelphia, Pennsylvania, issued a waiver to permit a photoless identification badge for a DLA employee working at DSCP who objected for religious reasons to having his photograph taken and displayed on the identification badge. In June 2005, the Naval Support Activity, Philadelphia reissued the DSCP employee a photoless Navy identification badge that did not comply with existing Naval Support Activity Instruction 5530.1. In 2006 DLA, without proper approval, provided the DSCP employee with an alternate method to access DoD networks and information systems, violating DoD and DLA policy. DLA revised its certificate practices policy to allow an individual without photo identification to access DoD networks in February 2008. DoD has not confiscated the photoless identification because of concerns about litigation under the Religious Freedoms Restoration Act. We discovered that the DSCP employee with the photoless identification used different Social Security numbers for a background investigation and logical access to DoD information systems. Therefore, we made a referral for investigation.

DoD has not approved guidance that prohibits issuance of photoless identification credentials, nor has DoD established a process to evaluate waiver requests. The issuance of a photoless identification card establishes a precedent that is contrary to the goal of

HSPD-12 to enhance security and could expose DoD installations and information systems to unauthorized access and potential terrorist exploitation.

Conclusion

The elimination of multiple forms of identification used to gain access to Federal facilities where there is potential for terrorist attacks is central to Federal Homeland Security policy to promptly field a secure and reliable Government-wide identification credential. The identification credential will allow security personnel and information systems to authenticate the identities of Federal Government employees and contractors before authorizing physical or logical access to Federal installations and information systems. DoD has not issued the necessary guidance to DoD Components to ensure that they are implementing the requirements of HSPD-12, which are designed to increase security for DoD installations and information systems, protect the privacy of DoD employees and contractors, and promote Government efficiency.

Recommendations, Client Comments, and Audit Response

Recommendations B.1. and B.2.a. have been revised in response to management comments and to clarify the intent of the recommendations.

B.1. We recommend that the Under Secretary of Defense for Personnel and Readiness develop and issue within 3 months a Deputy Secretary of Defense Directive to achieve full Department of Defense compliance with the requirements of Homeland Security Presidential Directive-12. The Directive should assign clear responsibility for compliance with each aspect of HSPD-12 and specify milestones for achieving compliance.

Client Comments. “OUSD (P&R) concurs with this recommendation. DoD is working from the January 2008 DoD HSPD-12 Implementation Plan which outlines the Department’s milestones for meeting those Federal conformance and interoperability capabilities we have agreed to support. However, OUSD (P&R) recognizes the need to coordinate additional milestones for areas that fall under the purview of other OSD PSAs (i.e., personnel security / background vetting). OUSD P&R will work with these organizations within the next three months to identify milestones that can be incorporated into the DoD HSPD-12 Implementation Plan.”

Audit Response. Client comments are not responsive. The intent of the original recommendation, as recognized by the client response, was that comprehensive DoD guidance be issued establishing clear areas of responsibility and milestones for implementation of HSPD-12. We request that the OUSD (P&R) respond to the revised recommendation, providing an anticipated completion date for corrective action.

B.2. We recommend that, within 3 months, the Under Secretary of Defense for Personnel and Readiness and the Under Secretary of Defense for Intelligence:

a. Revise DoD Directive 1000.25, “DoD Personnel Identity Protection (PIP) Program,” DoD Instruction 5200.08, “Security of DoD Installations and Resources,” DoD Regulation 5200.08-R, “Physical Security Program,” and other DoD issuances as necessary to appropriately reflect responsibility for incorporating FIPS 201-1 minimum requirements in all DoD electronic access control systems.

Client Comments (OUSD [P&R]). “OUSD (P&R) defers on a response to this recommendation; the responsibility for incorporating the minimum requirements for electronic access control systems does not fall under the purview of OUSD (P&R). OUSD (I) is the DoD lead for Physical Security to include the standards for access control. OUSD (P&R) will cooperate fully to support OUSD (I) with the development of these requirements and recommends that any subsequent guidance be incorporated within force protection or physical security publications or issuances such as the DoD Regulation 5200.8R issued by OUSD (I).”

Audit Response. The intent of the original recommendation was that DoD electronic access control systems used to identify personnel requiring routine access to DoD installations be compliant with FIPS 201-1 minimum requirements. USD(P&R) is the staff proponent for DoD Directive 1000.25, and USD(I) is the staff proponent for DoD Instruction 5200.08 and DoD Regulation 5200.08-R. We request that the OUSD(P&R) respond to the revised recommendation, providing an anticipated completion date for corrective action.

Client Comments (OUSD [I]). “OUSD (I) nonconcur. P&R is not the Principal Staff Assistant for Security, Access Control or Physical Security Equipment, which includes electronic access control systems. DoDD 1000.25 must be revised to delete all references to same. DoDI 5200.8 and DoDD 5200.8R will be revised to require all electronic access control systems to meet HSPD 12 and OMB guidance. OUSD(I) will coordinate with OSD (AT&L) to exercise RDT&E of all procurements for electronic access control systems in coordination with the Components physical security representatives and electronic systems engineers. OUSD(I) will maintain oversight in accordance with DoD Instruction 5143.01.”

Audit Response. Client comments are not responsive. The intent of the original recommendation was that DoD electronic access control systems used to identify personnel requiring routine access to DoD installations be compliant with FIPS 201-1 minimum requirements. USD(P&R) is the staff proponent for DoD Directive 1000.25, and USD(I) is the staff proponent for DoD Instruction 5200.08 and DoD Regulation 5200.08-R. We request that the USD(I) respond to the revised recommendation, providing an anticipated completion date for corrective action.

b. Develop minimum background check requirements for vetting foreign nationals in countries where no international security agreement exists, such as Iraq and Afghanistan.

Client Comments (OUSD [P&R]). “OUSD (P&R) defers on a response to this recommendation; the responsibility for personnel security standards does not fall under the purview of OUSD (P&R). OUSD (I) is the DoD lead for Personnel Security to include the standards for equivalent HSPD-12 vetting for Foreign Nationals. OUSD (P&R) will fully cooperate with OUSD (I) on incorporating identified requirements into the card issuance process and associated guidance.”

Audit Response. The client deferred to the OUSD (I) for comments on this recommendation.

Client Comments (OUSD [I]). “OUSD (I) concurs. The Department (CI&S), in conjunction with the Federal Interagency Working Group and with USD (Policy), ASD (International Security Affairs) is working to define an acceptable vetting process for foreign nationals requiring a CAC or physical access only badge in countries where no international security agreement has been established.”

Audit Response. Client comments are responsive.

B.3. We recommend that the Under Secretary of Defense for Intelligence:

a. Revise DoD Regulation 5200.08-R, “Physical Security Program,” April 9, 2007, within 3 months to:

(1) Require all contractors and Federal employees requiring routine physical access to a DoD installation to undergo a NACI background investigation and receive a DoD PIV credential.

Client Comments. “OUSD(I) concurs.”

Audit Response. Client comments are partially responsive. The Director did not indicate what actions he has taken or will take to accomplish the recommendation or include the anticipated completion date for corrective action. We request that the USD(I) provide additional comments on actions taken.

(2) Expressly prohibit the issuance of photoless identification credentials used to gain access to DoD installations and facilities, or establish a formal process to waive requirements for a photo on the credential.

Client Comments. “OUSD (I) concurs in part. OSD (P&R) is the proponent for CAC and Identification Card issuance. OUSD (I) is the proponent for physical access only credentials and will issue guidance to incorporate requirements mandated by Section 1069 of the 2008 National Defense Authorization Act. OUSD (I) will incorporate in policy procedures that “unescorted” access will not be granted for persons who do not present a photo identification credential. The federally compliant PIV credential and any physical access only credential will be required to be displayed as a visual access badge. Reasonable accommodation may be made for persons without photo identification, which will include “escorted” access, if an escort is available.”

Audit Response. Client comments are partially responsive. USD(I) did not specify the formal process to be established to waive requirements for a photo on the credential. We request that the USD(I) provide additional comments, including an anticipated completion date for corrective action.

(3) Delete paragraph C3.3.2 in its entirety and delete the reference to the Defense Biometric Identification System credential in paragraph C3.3.3 of the Installation Access section.

Client Comments. “OUSD (I) concurs. OUSD (I) has incorporated this stipulation in formally staffed draft policy, Directive Type Memorandum 08-004, Policy Guidance for DoD Access Control, which is pending USD (I) signature as of this submission and has added language that all upgrades or procurement of access control systems be FIPS 201 compliant.”

Audit Response. Client comments are responsive.

Client Comments (ASD[NII]/CIO). Although not required to comment, the Deputy Assistant Secretary of Defense for Information and Identity Assurance replied for the ASD(NII)/CIO. He stated: “It is documented that the Defense Biometric Identification System (DBIDS) was originally developed to meet a specific physical access credential requirement in EUCOM and PACOM prior to the issuance of HSPD-12. The vetting requirements included in the original DBIDS credential issuance process were specifically suited for populations of people that were not going to be eligible for a PIV-compliant credential. The DBIDS credential provided overseas commanders with a physical access only credential that raised the level of protection afforded to physical facilities while complying with best practices for electronically authenticated credential use. No where in the text of this report is it acknowledged that the HSPD-12 mandate and FIPS 201 identity credential standard does not apply to populations of personnel, other than employees or contractors, that have a legitimate requirement to access Federal installations or facilities on a routine or intermittent basis. DBIDS can meet the security, vetting, revocation and tracking requirements for populations such as volunteers, maintenance and supply vendors, unpaid interns, employees of non-military concessions and businesses operating within installations or facilities. Recommend removing Recommendation B.3.a.(3) from the report.”

Audit Response. We reviewed client comments and determined that report revisions were not required. USD(I) has responsibility for DoD physical access control policy and has stated that DoD Regulation 5200.08-R will be revised to remove paragraph C3.3.2 in its entirety.

b. Suspend use of the Defense Biometric Identification System and any other alternative credentials not explicitly approved by the Under Secretary of Defense for Intelligence for physical access to DoD installations and facilities.

Client Comments (OUSD [I]). “OUSD (I) concurs in part. OUSD (I) will not suspend use of existing legacy access control systems, which includes DBIDS until such time as we have identified, tested and certified a replacement or upgrade that meets FIPS 201, Security Equipment Integration and network security requirements. Suspending use of existing legacy access control systems, whether FIPS compliant or not, would degrade the only security mitigators we have in place at the present time. The Directive Type Memorandum 08-004, Policy Guidance for DoD Access Control will require Heads of DoD components when purchasing upgrades to existing access control systems or when replacing current systems, the upgraded system must meet FIPS 201 (including ISO [International Organization of Standardization] 14443 contactless technology and ability

to perform automated personal identity verification); include an emergency power source; and have the ability to provide rapid electronic authentication to Federal and DoD authoritative databases, including DoD personnel registered in the Defense Enrollment and Eligibility Reporting System. This change in policy will prohibit the procurement of non FIPS 201 compliant systems.”

Audit Response. Client comments are responsive.

Client Comments (OUSD [P&R]). Although not required to comment on this recommendation, the USD(P&R) provided these comments. “OUSD (P&R) non-concurs with the recommendation to suspend the use of the Defense Biometric Identification System (DBIDS). This access control system is installed throughout Europe, Korea, Japan, Guam, the AOR [area of responsibility] (except Iraq and Afghanistan) and some locations in CONUS [the continental United States], for a total of 157 bases. The use of this system has substantially increased security at each of the bases where it is used compared to the historical use of “flash and pass” processes. To suspend usage of this system would significantly degrade security at each of these bases where it is currently operating or defer improvement in security at those bases where DBIDS implementations are planned. OUSD (P&R) would concur with a recommendation that DBIDS migrate to meet the policy published by OUSD (I).”

Audit Response. USD(I) has responsibility for DoD physical access control policy and has stated that his office will not suspend use of legacy access control systems including DBIDS. The USD(I) will require heads of DoD Components to meet FIPS 201-1 requirements when updating or replacing existing access control systems.

Appendix A. Scope and Methodology

We performed this audit from March 2007 through February 2008 in accordance with generally accepted government auditing standards. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. The evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We evaluated the implementation of HSPD-12; Federal Information Processing Standards Publication 201-1; OMB Memorandums M-05-24 and M-07-06, National Institute of Standards and Technology Special Publications 800-73-1, 800-85A and B, and 800-79; and DoD Regulation 5200.08-R. We interviewed personnel and obtained information from staff at DMDC, Defense Human Resources Activity, Pentagon Force Protection Agency, Public Key Infrastructure Program Management Office, Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer; Under Secretary of Defense for Acquisition, Technology, and Logistics, Under Secretary of Defense for Intelligence, General Services Administration, and RAPIDS workstations site security managers, physical security officials, and human resources personnel with the Departments of the Army, Navy, Air Force, Marine Corps, Coast Guard, and the Defense Logistics Agency.

We visited the DMDC West facility to determine the stage of HSPD-12 compliance and to review CAC testing, issuance, and infrastructure. We judgmentally selected several military and Coast Guard installations with CAC issuance facilities to determine HSPD-12 compliance at the installation level.

- Camp Parks, San Francisco, California
- Fort Hunter Liggett, Monterey, California
- Moffett Field, Mountain View, California
- Presidio of Monterey, Monterey, California
- Naval Postgraduate School, Monterey, California
- Navy Yard, Washington Navy Yard, Washington, D.C.
- Customer Service Desk, Monterey, California
- Travis Air Force Base, San Francisco, California
- Andrews Air Force Base, Maryland
- Onizuka Air Force Base, Sunnyvale, California
- Marine Corps Base Quantico, Quantico, Virginia
- Alameda Coast Guard Support Center, Alameda, California
- Petaluma Coast Guard Training Center, Petaluma, California
- Defense Logistics Agency, Fort Belvoir Army Base, Fort Belvoir, Virginia
- Defense Logistics Agency, Defense Supply Center, Naval Support Activity, Philadelphia, Pennsylvania

These installations were selected because of their close proximity to DMDC West or the National Capital Region, their participation in beta testing the RAPIDS 7.2 software, and the variety of services they provide. We visited the Defense Supply Center-Philadelphia and Defense Logistics Agency because we received a referral from the Defense Criminal Investigative Service, Philadelphia regarding a photoless identification cardholder at the Defense Supply Center-Philadelphia. At all locations, we observed the CAC issuance process, inquired about physical security measures for the base as well as securing the inventory of CAC card stock, asked about training requirements for staff involved in CAC card issuance and inquired about the human resources process pertaining to background checks.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Use of Technical Assistance

Members of the Technical Assessment Directorate assisted the auditors in understanding technical aspects of the audit. Mr. Jaime Bobbio, electronics engineer, and Mr. Minh Tran, computer engineer, helped in the review of technical guidance, tests of technology on cards, and the understanding of how the next-generation CAC will work.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) has issued two reports discussing Federal Employee Identification Standards. Unrestricted GAO reports can be accessed over the Internet at <http://www.gao.gov>.

GAO

GAO Report No. 08-120SU, "Military Bases, High-level Access Control Guidance Is Consistent, but Flexible For Local Circumstances and Evolving to Standardize Access Control," October 2007.

GAO Report No. 06-178, "Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard," February 2006.

Appendix B. Guidance on Identification and Access Control

Public Law

Public Law 109-364, “John Warner National Defense Authorization Act for Fiscal Year 2007, Section 585,” October 17, 2006, requires that no later than 180 days after the enactment of this Act, the Secretary of Defense shall submit to Congress an assessment of the feasibility of utilizing military identification cards that do not contain, display, or exhibit the Social Security number of the individual identified by a military identification card.

The Privacy Act of 1974 was created in response to concerns about how the creation and use of computerized databases might affect individuals’ privacy rights. It safeguards privacy by creating four procedural and substantive rights regarding personal data. First, it requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called “fair information practices,” when gathering and handling personal data. Third, it restricts how agencies can share an individual’s data with other people and agencies. Fourth and finally, it permits individuals to sue the Government for violating Privacy Act provisions.

Congressional Language

H.R. REP. NO. 109-452, 109th Cong., 2nd Sess. (May 5, 2006), “National Defense Authorization Act for Fiscal Year 2007 Report of the Committee on Armed Services House of Representative on H.R. 5122 together with Additional and Dissenting Views,” directed the Secretary of Defense to study the feasibility of developing an alternative process that would allow service members to immediately request that their military identification cards not include their Social Security number.

Presidential Directive

Homeland Security Presidential Directive-12, “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 27, 2004, states that wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, the President stated that it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. To implement the policy, the Secretary of Commerce shall promulgate a Federal standard for secure and reliable forms of identification no later than 6 months after the date of HSPD-12 in consultation with the Secretaries of State, Defense and Homeland Security; the Attorney General; the Director of the Office of Management and Budget, and the Director of the Office of Science and Technology Policy. For purposes of this directive, secure and reliable forms of identification are issued based on sound

criteria for verifying an individual employee's identity; strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation, can be rapidly authenticated electronically, and is issued only by providers whose reliability has been established. In addition, no later than 4 months following promulgation of the standard, the heads of executive departments and agencies shall have a program in place to ensure the identification issued by their departments and agencies to Federal employees and contractors meets the standard. Additionally, the heads of executive departments and agencies shall require the use of identification by Federal employees and contractors that meets the standard in gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems.

OMB Memoranda

OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007, requires agencies to eliminate the unnecessary use of the Social Security number. Agencies must now also review their use of the Social Security number in agency systems and programs to identify instances in which collection or use of the Social Security number is superfluous. The memo indicates that, within 120 days of the date of the memo, agencies must establish a plan to eliminate the unnecessary collection and use of the Social Security number within 18 months.

OMB M-07-06, "Validating and Monitoring Agency Issuance of Personal Verification Credentials," January 11, 2007, discusses validating and monitoring agency issuance of PIV-compliant identity credentials in support of HSPD-12. Additionally, OMB M-07-06 directed all agencies to provide GSA a credential with their agency's standard configuration by January 19, 2007.

OMB M-06-18, "Acquisition of Products and Services for Implementation of HSPD-12," June 30, 2006, provides updated direction for the acquisition of products and services for the implementation of HSPD-12 and the status of implementation efforts.

OMB M-05-24, "Implementation of Homeland Security Presidential Directive-12 Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005, requires development and agency implementation of a mandatory, Government-wide standard for secure and reliable forms of identification for Federal employees and contractors. It also establishes timelines and milestones for FIPS 201-1 compliance.

NIST Directives and Special Publications

Federal Information Processing Standards Publication 201 (FIPS 201), "Personal Identity Verification (PIV) of Federal Employees and Contractors," February 25, 2005, provides standards for the identity verification, issuance, and use of the common identity standard. It contains two major sections. Part One describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. Part Two provides detailed specifications that will support technical interoperability of PIV systems of Federal departments and agencies. It describes the card elements, system

interfaces, and security controls required to securely store, process, and retrieve personal identity information from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard.

FIPS PUB 201-1, Change Notice-1 (FIPS 201-1) “Personal Identity Verification of Federal Employees and Contractors,” March 2006, updates the requirements established by FIPS 201. Specifically, it makes changes to the graphics on the back of the PIV card and the Abstract Syntax Notation One encoding of the NACI indicator.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-85B, “PIV Data Model Test Guidelines,” July 2006, provides technical guidance on the methodology to be used during testing applicable components and specifies the derived test requirements, detailed test assertions, and conformance tests for testing the data elements of the PIV system.

NIST SP 800-85A, “PIV Card Application and Middleware Interface Test Guidelines,” April 2006, provides test requirements and test assertions that could be used to validate the compliance/conformance of two PIV components—PIV middleware and PIV card application to specifications in NIST SP 800-73.

NIST SP 800-73-1, “Interfaces for Personal Identity Verification,” March 2006, contains technical specifications for the smart card, the interface, the manner in which data on the credential are protected, and the format in which the data are to be retrieved. These specifications reflect the design goals of interoperability and PIV card functions.

DoD Regulation

DoD Regulation 5200.08-R, “Physical Security Program,” April 9, 2007, issued under the authority of DoD Instruction 5200.08, implements the policies and minimum standards for the physical security of DoD installations and resources. This regulation applies to all organizational entities in the Department of Defense, referred to collectively as “DoD Components,” and is mandatory. This regulation addresses the physical security of personnel, installations, facilities, operations, and related resources of DoD Components, and provides minimum standards for the protection of resources normally found on installations. Regulation objectives include standardizing personal identification authentication for DoD installations and facilities, promoting interoperability with other Federal entities, and utilizing the DoD PIV credential as the universal authority of individual authenticity. The DoD PIV credential will provide the level of identity assurance and Government-wide recognition mandated by HSPD-12. The regulation also establishes DBIDS as an alternative to the CAC.

DoD Directives

DoD Directive 1000.25, “DoD Personnel Identity Protection (PIP) Program,” July 19, 2004, establishes policy for the implementation and operation of the PIP program including use of identity information, issuance and use of DoD identity credentials, and operation of the Defense Enrollment and Eligibility Reporting System, Real-time Automated Personnel Identification System (RAPIDS) and associated systems, DBIDS,

Defense Cross-Credentialing Identification System, Defense National Visitors Center, and the Defense Noncombatant Evacuation Operations Tracking System.

DoD Directive 8190.3, “Smart Card Technology,” August 31, 2002, requires that smart card technology applied in the form of a CAC shall be the standard identification card and the Department’s primary platform for the Public Key Infrastructure (PKI) authentication token used to access DoD computer networks and systems.

DoD Instructions

DoD Instruction 8520.2, “Public Key Infrastructure and Public Key Enabling,” April 1, 2004, assigns responsibility to the ASD(NII/CIO) to serve as the Designated Approving Authority for the DoD PKI; approve or disapprove Department-wide waivers submitted by the DoD PKI Program Management Office; and approve DoD use of hardware tokens other than the CAC for identity, signature, and encryption certificates. The DoD Component CIOs shall have responsibility to approve or disapprove waiver requests in accordance with waiver process guidance and to submit approved waivers to the ASD(NII/CIO). The Director, DoD PKI Program Management Office, is to review justification of requests for hardware tokens other than the CAC for identity, signature, and encryption certificates and provide a recommendation for action to the ASD(NII/CIO). The instruction also requires authentication with certificates issued by the DoD PKI on hardware tokens. A hardware token is defined as a portable, user-controlled, physical device used to generate, store, and protect cryptographic information and to perform cryptographic functions.

DoD Instruction 1000.1, “Identity Cards Required by the Geneva Conventions,” January 30, 1974, provides requirements for the form, issuance, and use of identity cards required by the Geneva Conventions of August 12, 1949, for the protection of war victims.

DoD Memoranda and Task Orders

DoD Memorandum, “Discontinuance of Military Service Number as Personnel Identification,” January 1967, authorizes the substitution of the Social Security number for the military service number on ID badges and tags throughout DoD when a unique identification of individuals is required.

USD(P&R) Memorandum, “Common Access Card (CAC) Eligibility for Foreign National Personnel,” March 9, 2007, applies to DoD-sponsored foreign national military, government and contractor personnel who are sponsored by their government as part of an official visit or assignment to work on a DoD installation or controlled space or requiring access to DoD networks both on site or remotely.

The Joint Task Force Global Network Operations (JTF-GNO) Communications Task Order 06/02, “Tasks for Phase 1 of the Accelerated Public Key Infrastructure (PKI) Implementation,” January 2006. The task order states that, upon receipt, all DoD Components are directed to accelerate PKI implementation. It explains that ongoing intrusion activity has focused on exfiltration of valid usernames and passwords for use in

further exploitation and access, presenting a direct danger to the Global Information Grid. Task three requires 100-percent compliance with smart card log-on to the NIPRNET using DoD PKI for all Components no later than July 31, 2006. This task applies specifically to the ability to log on to the network, and applies to all desktops, servers, and laptops that connect to the NIPRNET.

JTF-GNO Communications Task Order 06/02 Update #3, “Focused Effort to Secure NIPRNet Web Servers,” September 21, 2006, provides notice to DoD Components of enforcement measures to ensure proper configuration of private DoD Web servers and eliminate all username/password and non-DoD PKI certificate authorities. Task two requires that all Components allow only certificate-based client authentication to private DoD Web servers using certificates issued by DoD PKI certificate authorities. These actions will affect mission and mission-support systems that are not PKI compliant as well as people who do not have CACs who may require access to PKI-authenticating systems. Individuals without CACs must use either an alternate log-on token or another approved method of two-factor authentication. Exceptions will be based on valid operational needs, and approved exceptions must be submitted to the JTF-GNO and must include a Plan of Action & Milestones for mitigation or completion, as well as a statement of operational risk.

Military Department Directive

Department of the Navy, Naval Support Activity (NSA) Instruction 5530.1, “Identification Badges and Passes for Entrance onto the NSA Philadelphia Compound,” May 31, 1991, states that civilian employees are required to wear ID badges at all times while on the compound. When entering the compound, pedestrian employees must present their ID badge to the guard to verify the photo and expiration date.

DoD Component Instruction

Defense Logistics Agency Instruction (DLAI) 5710.1, “Physical Security Program,” August 12, 1994, prescribes procedures and minimum standards for the physical protection of DLA personnel, installations, operations, and assets. The instruction states that all DLA activities will establish procedures for the identification and control of personnel and visitors. The DLA ID card is issued to DLA employees and is not meant to grant access to security areas; a separate key card or badge should be issued for this purpose. The card configuration example indicates that a photo of the cardholder is to be displayed in the lower left corner of the card. At a minimum, the front of the badge must contain a color photograph; a serial number; issuing activity; the signature of the authenticating official; the signature, name, organization, and height of the holder; and the expiration date of the badge. ID badges for permanent DLA employees and tenant activity personnel bear an expiration date that is no more than 5 years from date of issue.

Appendix C. Client Comments on the Findings and Audit Response

USD(P&R) Comments on the Findings

The Deputy Under Secretary of Defense (Program Integration) responded for the USD(P&R). Below are excerpts from the draft report, clarifications that the USD(P&R) recommended, and audit responses.

Item 1 (page 2, “Background”)

Excerpt: “As of March, 2007, DoD has issued 56 such credentials.”

Client Comments. “As outlined in our March 2008 PIV issuance report to OMB, DoD has issued 108,778 PIV transitional configured CACs.”

Audit Response. We reviewed client comments and determined the draft report was accurate. According to the Department of Defense Status Report updated December 26, 2007 (downloaded from the Defense Manpower Data Center Web site as of March 2007), DoD had issued 56 PIV cards to employees. The Department of Defense Status Report updated April 1, 2008, cites 83,659 PIV cards issued for employees and 25,119 PIV cards issued for contractors, totaling 108,778 PIV cards. We have updated the report to reflect the transitional PIV cards issued after the draft report.

Item 2 (page 2, “Internal Controls”)

Excerpt: “Implementing the recommendations made in this report, together with those developed for a related audit, Project No. D2007-D000LA-0199, ‘Controls Over the Contractor Common Access Card Life Cycle,’ will assist in bringing the Department into compliance. A copy of the final report will be provided to the senior official responsible for internal controls in DoD.”

Client Comments. “It is inappropriate to reference an incomplete audit which draft results have not been shared with organizations engaged with the audit. DoD IG recommendations and findings related to Project No. D2007-D000LA-0199 should be addressed by a separate audit through the formal audit review processes.”

Audit Response. Both reports pertain to transitional PIV cards, and common internal control weaknesses should be addressed together. Results of Project D2007-D000LA-0199 were shared with OUSD(P&R) on April 15, 2008, however, the results have not yet been published and, therefore, the reference has been deleted.

Item 3 (page 3, “DoD Implementation of HSPD-12”)

Excerpt: “DoD failed to meet the milestones approved by the Office of Management and Budget (OMB) in 2005 for compliance with HSPD-12 by 2010.”

Client Comments. “DoD has updated its original HSPD-12 Implementation Plan to OMB on two occasions (most recently 24 January 2008). OMB approved our initial revision (September 2006) and is currently reviewing our January 2008 revision.”

Audit Response. We reviewed client comments and determined that report revisions were not required. Auditors requested supporting documentation for the OUSD(P&R) assertion that OMB approved the DoD HSPD-12 Implementation Plan revision of September 2006; the requested support was not provided. Further, the September 2006 revision projected PIV-II transitional initial operational capability would be attained by October 27, 2006, and full HSPD-12 compliance 3.5 years later (2010). Neither projection will be realized. The most recent DoD HSPD-12 Implementation Plan of January 24, 2008, projects full compliance with HSPD-12 by the summer of 2012.

Item 4 (page 5, “Deadlines for Completion of Background Checks”)

Excerpt: “According to DoD’s January 2008 implementation plan, as of December 26, 2007, the following numbers of DoD employees and contractors have not completed the required background checks: Military/Civilian (1,240,214); contractors (196,185); total (1,436,399).”

Client Comments. “The numbers provided within the DoD’s January 2008 Implementation Plan reflected efforts taken to reconcile CAC issuance records with JPAS. The 1,436,399 number are records that showed as ‘unknown’ during this effort, but does not mean that these individuals do not have background investigations. The use of the term ‘have not completed’ is not accurate.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The numbers reported in the Implementation Plan were identified as Federal civilian, military, and contract employees requiring NACI or equivalent background checks that had not previously undergone a NACI. The report noted, as did the January 24, 2008, DoD Implementation Plan, that the numbers might not be accurate due to JPAS data quality.

Item 5 (page 5, “Privacy Requirements”)

Excerpt: “DoD Geneva Conventions credential for members of the uniformed service does not comply with HSPD-12 or with Federal policies and requirements to reduce identity fraud and protect personal privacy.”

Client Comments. “The DoD Geneva Conventions CAC does comply with standards issued for HSPD-12 (see FIPS 201-1, Section 4.1.4.4, page 20).”

For Zones 9 and 10, departments and agencies are encouraged to use this area prudently and minimize printed text to that which is absolutely necessary.

In the case of the Department of Defense, the back of the card will have a distinct appearance. This is necessary to display information required by Geneva Accord and to facilitate medical entitlements that are legislatively mandated.

“The additional references in the ‘Privacy Requirements’ section regarding Social Security Numbers (SSN) are not specifically related to HSPD-12, associated NIST publications, and relevant OMB memoranda (M05-24) on HSPD-12. In fact, the Administration’s initiative to reduce the use and exposure of SSN within the Federal Government began in April 2007 with the release of the Presidential Task Force on Identity Theft’s strategic plan (and subsequent OMB memo M07-16 22 May 2007). Until FIPS 201-1 is updated to align with new Federal policies related to SSNs, this topic is outside the scope of the audit announcement.

DoD has engaged in the effort to decrease the possibility of our Service members exposure to identity fraud/theft through the Department’s use of SSN. USD (P&R) provided a Report to Congress that outlines the Department’s plan. We have been working to secure consensus with others within the Department and adjust the necessary paperwork to make sure our proposal satisfies the Geneva Conventions requirements. A directive-type memorandum, ‘DoD Social Security Number Reduction Plan,’ was signed by USD (P&R) 29 March 2008.”

Audit Response. We reviewed client comments and determined that report revisions were not required. HSPD-12 policy specifically mandates the protection of personal privacy and the reduction of identity fraud by establishing a standard for secure and reliable forms of identification. Secure and reliable forms of identification are defined in part as being strongly resistant to identity fraud. The printing of the entire Social Security number on PIV credentials does not comply with the objective of HSPD-12 to reduce the potential for identity theft. To suggest otherwise is inconsistent with presidential and congressional direction to protect personal privacy.

FIPS 201-1 contains Geneva Conventions card requirements for zones 9 and 10. FIPS 201-1 encourages that agency-specific text in zones 9 and 10 of PIV cards be limited to text that is absolutely necessary. The printing of the entire Social Security number on Geneva Conventions cards should be discontinued. The Department’s plan to truncate the visible Social Security number on Geneva Conventions credentials to four digits will reduce the potential for identity theft. The directive-type memorandum signed by the USD(P&R) was issued after publication of this draft report. During the formal comment period, the DoD Inspector General did not concur.

Item 6 (page 5, “Privacy Requirements”)

Excerpt: “No time table was provided to implement the recommendation, however, nor did the report specify who was responsible for implementation.”

Client Comments. “Identification cards to support Geneva Conventions and benefits/eligibility are clearly the responsibilities of the USD (P&R). Authorship of the report to Congress, ‘Omission of the SSN from the Department of Defense Military Identification Cards,’ May 23, 2007, was led by the OUSD (P&R) and signed by USD (P&R).”

Audit Response. We reviewed client comments and determined that report revisions were not required. We agree identification cards to support Geneva Conventions and benefits and eligibility are clearly the responsibilities of USD(P&R); however, the report to Congress does not explicitly state which DoD Component is responsible for implementing the recommendations.

Item 7 (page 6, “Personal Identity Verification-II Requirements”)

Excerpt: “DoD did not meet the March 2006 PIV-II initial operating capability implementation milestone approved by OMB in the DoD implementation plan, nor did DoD meet the October 2006 OMB milestone for final PIV-II implementation.”

Client Comments. “The reference for the March 2006 PIV-II IOC [initial operational capability] date is unclear. The approved DoD HSPD-12 Implementation Plan states the following:

- DoD achieved “initial operational capability (IOC) for PIV I” by October 27, 2005.
- DoD achieved “IOC for PIV II” with issuance of DoD PIV transitional cards by October 27, 2006.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The DoD HSPD-12 Implementation Plan of June 27, 2007, projected PIV-II initial operational capability would be achieved within 9 to 12 months of promulgation by the National Institute of Standards and Technology (NIST) of the required information and the availability of production-quality products that support PIV-II. NIST Special Publication 800-73, “Interfaces for Personal Identity Verification,” was promulgated in April 2005. March 2006 was the 12-month point for the DoD projected PIV-II initial operational capability. In addition, OMB Memorandum M-05-24, “Implementation of Homeland Security Presidential Directive (HSPD)-12, “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 5, 2005, required all agencies to begin compliance with PIV-II by October 27, 2006. DoD was not and is not compliant with PIV-II because DoD’s PIV credential is missing at least two key elements of PIV-II: (1) the mandatory PIV PKI authentication certificate and (2) the DoD PIV applet.

Item 8 (page 8, “DoD Transitional Credential”)

Excerpt: “. . .workstations to RAPIDS version 7.2 to produce DoD PIV credentials for DoD installations in the continental United States by December 12, 2008. No schedule for deployment of updated RAPIDS workstations has been announced for four installations outside the continental United States, including two in Germany and one each in Djibouti and Greenland.”

Client Comments. “The RAPIDS upgrade schedule to produce DoD PIV credentials for calendar year 2008 includes all OCONUS installations in Europe, Africa, and Asia, including those referenced in the excerpt. The only workstations that it does not include are those portable deployable shipboard and forward deployed units. OUSD (P&R) is

working directly with the Services to upgrade these workstations as they return from theater or deployment or have a period of availability.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The installation schedule does include these four locations. However, the notation in the columns “install begin” and “install end” for the two Germany locations is “TBD [to be determined].” Therefore, they are not considered scheduled. The “install begin” column contains dates for Djibouti and Greenland. However, the “install end” column indicates “TBD.”

Item 9 (page 11, “DoD Component Implementation Efforts”)

Excerpt: “Components have been authorized to issue Defense Biometric Identification System (DBIDS) credentials instead of PIV credentials.”

Client Comments. “DBIDS is a local or regional perimeter access control system that uses the CAC (for those individuals who qualify) and contains local physical access only badging capabilities (for those who do not qualify for a CAC). DBIDS credentials are not issued to those who possess CACs. As such, HSPD-12, associated NIST publications, and relevant OMB memoranda (especially M05-24) on HSPD-12 have nothing to do with DBIDS. This topic is outside the scope of the audit announcement, ‘DoD Implementation of Homeland Security Presidential Directive-12.’”

Audit Response. We reviewed client comments and determined that report revisions were not required. As stated in the draft report, contractors requiring access to DoD facilities and installations for more than 6 months receive DBIDS cards. As stated in OMB Memorandum M-05-24, these contractors must receive a PIV credential and are subject to the HSPD-12 required vetting process. In addition, OMB Memorandum M-05-24 does not differentiate between physical access to a single facility and physical access to multiple facilities.

Item 10 (page 12, “Photoless Identification”)

Excerpt: “The Commanding Officer at the Naval Support Station (now Naval Support Activity) in Philadelphia, Pennsylvania, issued a waiver for a photo identification badge to a Defense Logistics Agency (DLA) employee working at Defense Supply Center-Philadelphia (DSCP) who objected for religious reasons to having his photograph taken and displayed on the identification badge.”

Client Comments. “The badge in questions is not a CAC. It was a locally issued badge to facilitate access to the installation. A congressional response dated October 16, 2006 stated that a special exemption to policy could not be approved through OUSD (P&R), to receive a CAC without a picture, but if the religion could be accommodated in another way, then OUSD (P&R) could waive the requirement to receive a CAC. This is the only documented request across 3.5 million active CACs.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The audit report clearly states that the credential is a Navy

identification badge, and does not imply that it is a CAC. The congressional response dated October 16, 2006, does clearly state that a CAC cannot be issued without a photo, but it makes no mention of alternative religious accommodation or of waiving the requirement to receive a CAC.

Item 11 (page 12, “DBIDS Credentials”)

Excerpt: “DoD has authorized Components to issue a DBIDS card to employees and contractors who require only routine physical access. This practice deviates from HSPD-12.”

Client Comments. “DBIDS cards are not issued to DoD civilian or military personnel—those individuals receive CACs. Identification of those contractors who are to receive a PIV card is based on the Department’s determination of the access requirement. DoD has defined eligible CAC contractors in the following manner in the draft ‘Next Generation CAC Implementation Guidance’ directive-type memorandum (DTM), signed into the SD 106 staffing process on 6 March 2008”:

CAC eligibility for other populations, including DoD contractors, non-DoD Federal civilians, state employees, and other non-DoD affiliates, is based on the government sponsor’s determination of the type and frequency of access required to DoD facilities or networks that will effectively support the mission. To be eligible for a CAC, the access requirement must meet one of the following criteria:

- The individual requires access to multiple DoD facilities or access to multiple non DoD Federal facilities on behalf of DoD (this requirement is applicable to DoD contractors only).
- The individual requires both access to a DoD facility and access to DoD networks on site or remotely.
- The individual requires remote access to DoD networks that use only the CAC logon for user authentication.

Audit Response. We reviewed client comments and determined that report revisions were not required. DoD Regulation 5200.08-R, “Physical Security Program,” April 9, 2007, does not specify the type of individuals who will receive a DBIDS card. Instead, the Regulation states that the “DBIDS card shall be issued and authorized for routine, physical access, to a single DoD installation or facility.” In addition, as the client’s comments state, the “Next Generation CAC Implementation Guidance” is a draft document.

Item 12 (page 12, “DoD HSPD-12 Policy and Guidance”)

Excerpt: “DoD established a working group to develop comprehensive guidance for implementation of HSPD-12, but the group has made only limited progress.”

Client Comments. “The HSPD-12 workgroup has made significant progress since its inception. A Deputy Secretary of Defense level Directive Type Memorandum (DTM) on HSPD-12 policy is in formal SD106 coordination. In addition, an SD 106 coordination request was signed by Dr. Chu for a DTM on the ‘Next Generation CAC Implementation Guidance’ on 5 March 2008. Additionally, several sub-working groups have been

established and are meeting to directly address issues regarding personnel security and vetting criteria in compliance with HSPD-12, and to set standards for access control to DoD installations and facilities.”

Audit Response. We reviewed client comments and determined that report revisions were not required. Members of the HSPD-12 working group expressed frustration with delays in formulating the implementation guidance because of Component disagreements and nonconcurrence regarding responsibility for implementation elements. On April 10, 2008, after issuing the draft report on March 21, 2008, the DoD Office of Inspector General received the Draft USD(P&R) Guidance, “Next Generation Common Access Card (CAC) Implementation Guidance in Support of Homeland Security Presidential Directive-12 (HSPD-12),” for coordination. On April 11, 2008, the DoD Office of Inspector General received for coordination the Draft Deputy Secretary of Defense Directive-Type Memorandum (DTM) #2008-006, “DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12).” Both documents remain in draft and under revision to address concerns of DoD Components other than USD(P&R).

Item 13 (page 12, “DoD HSPD-12 Policy and Guidance”)

Excerpt: “Meanwhile, DoD senior management chose to establish and implement less stringent access control requirements than those established by HSPD-12.”

Client Comments. “HSPD-12 associated NIST publications, and relevant OMB guidance do not provide specific mandates or timetable for the use of HSPD-12 credentials to control access to Federal network assets or installations. In fact, the CAC was implemented in 2000 and has provided a secure and reliable identification card prior to the release of HSPD-12 so that it is used daily to:

- Facilitate access to DoD facilities and installations around the world.
- Authenticate to 98% of the Department’s unclassified network accounts and 100% of the Departments private web servers, web sites, and portals. This has resulted in:
 - Successful intrusions declining **46 percent** in the past year because of a requirement that all DOD personnel log on to unclassified networks using CACs, although there are 6 million probes of Defense Department networks a day. (JTF GNO, Lt. Gen. Charles Croom, Federal Computer Weekly article on 25 January 2007)
 - The Number of successful socially engineered e-mail attacks (definition: A socially engineered attack is one in which the user is somehow tricked into doing the attacker’s bidding) against DoD users—a practice known as spear phishing—declining **30 percent** in the past year (JTF GNO, Lt. Gen. Charles Croom, Federal Computer Weekly article on 25 January 2007).”

Audit Response. We reviewed client comments and determined that report revisions were not required. DoD Regulation 5200.08-R, “Physical Security Program,” April 9, 2007, paragraph C3.3.2. and paragraph C3.3.3., establishes a less stringent access control requirement. DoD Regulation 5200.08-R requires the implementation of DBIDS throughout DoD installations and facilities. As stated in the draft report, DBIDS does not meet the HSPD-12 security and access control requirements. The Director of Security in the Office of the Under Secretary of Defense for Intelligence has agreed to revise and remove references to DBIDS from DoD Regulation 5200.08-R.

Item 14 (page 13, “Issuance of Guidance”)

Excerpt: “DoD Regulation 5200.08-R . . . is inconsistent with HSPD-12 because it allows DBIDS and other forms of identification that are not compliant with FIPS 201-1.”

Client Comments. “See remarks in item 16.”

Audit Response. See audit response for item 16.

Item 15 (page 13, “DBIDS Credential and Physical Access Control System”)

Excerpt: “OMB instructed agencies to be careful not to develop policies that contradict HSPD-12 standards for identity proofing and issuance of credentials. HSPD-12 standards mandate that all Federal employees and contractors requiring routine access for 180 days or greater receive a PIV-compliant credential and undergo a NACI or equivalent background check. DoD Regulation 5200.08-R authorizes personnel requiring only routine physical access to receive a DBIDS credential and undergo the less rigorous NAC. Granting routine access to DoD installations to personnel who have only a NAC background check does not fully comply with the HSPD-12 policy objective to enhance security and protect physical and human capital assets all DoD installations.”

Client Comments. “See remarks in item 16.”

Audit Response. See audit response for item 16.

Item 16 (page 13, “DBIDS Credential and Physical Access Control System”)

Excerpt: “Yet the system does not meet the minimum standards of FIPS 201-1 to verify the claimed identity of individuals seeking physical access to Federal Government facilities . . . DBIDS uses card readers and scanners that are not on the Approved Products List as required by OMB.”

Client Comments. “DBIDS is a local or regional perimeter access control system that uses the CAC (for those individuals who qualify) and contains local physical access only badging capabilities (for those who do not qualify for a CAC). DBIDS credentials are not issued to those who possess CACs. As such, HSPD-12, associated NIST publications, and relevant OMB memo on HSPD-12 have nothing to do with DBIDS. This topic is outside the scope of the audit announcement, ‘DoD Implementation of Homeland Security Presidential Directive-12.’”

Audit Response. We reviewed client comments and determined that report revisions were not required. According to DoD Regulation 5200.08-R, paragraph C3.3.2., “the DBIDS card renders a source of identity and verification of affiliation with the Department of Defense, and is a proven physical access system in accordance with Reference (r) [FIPS 201-1].” However, the DBIDS system does not meet the minimum standards of FIPS 201-1, as stated in the draft report. The policy of the Director of Security in the Office of the Under Secretary of Defense for Intelligence is that all upgrades and procurements of access control systems be FIPS 201-1-compliant.

Item 17 (page 13, “DBIDS Credential and Physical Access Control System”) Excerpt: “Neither the DBIDS system nor the card is configured to operate with HSPD-12 security features such as PKI certificates, the Card Holder Unique Identifier, and biometrics embedded in the integrated circuit chip of the credential.”

Client Comments. “See remarks in item #18.”

Audit Response. See audit response for item #18.

Item 18 (page 13, “DBIDS Credential and Physical Access Control Systems”) Excerpt: “Further, the use of barcode technology on the DBIDS credential does not enhance security because the barcode, a static physical card feature, cannot deter fraud, prevent counterfeiting, or protect privacy. . . . DBIDS does not meet the FIPS 201-1 minimum standards to enhance security, increase Government efficiency, and protect personal privacy.”

Client Comments. “See remarks in item #13. Additionally, individuals who receive local access badges or DBIDS credentials typically do not receive CACs (e.g., DoD PIV credential). There is no place within HSPD-12, FIPS 201 or OMB M05-24 that specifies access control rules/criteria for physical installations and/or IT assets covering personnel who do not qualify for CACs or Federal PIVs. The type of background investigations conducted on these individuals is outside the scope of HSPD-12.

Moreover, PKI is not intended to be used in the physical access control environment. DBIDS, which predates HSPD-12, is a complementary not competing system. DBIDS:

- Went operational on 9/11/2001 in Korea
- Was built to optimize interoperability through use of bar code technologies
- Managed risk by using local or regionally stored biometrics for authentication which minimizes risk of fake/fraudulent cards
- Is scalable to FPCON levels
- Is able to provide information sharing across a region.”

Audit Response. We reviewed client comments and determined that report revisions were not required. DoD Regulation 5200.08-R, “Physical Security Program,” April 9, 2007, paragraph C3.3.2. and paragraph C3.3.3., establishes a less stringent access control requirement. DoD Regulation 5200.08-R requires the implementation of DBIDS throughout DoD installations and facilities. The Director of Security in the Office of the

Under Secretary of Defense for Intelligence has agreed to revise and remove references to DBIDS from DoD Regulation 5200.08-R. In the draft report we address only contractors who qualify for a PIV credential but receive a DBIDS credential—for example, contractors who require only routine physical access to a single facility for 6 months or more and qualify for a PIV credential but are given DBIDS cards. In addition, FIPS 201-1 states the PIV card can be used to authenticate the cardholder in a physical access control environment.

Item 19 (page 14, “Photo Identification Requirements”)

Excerpt: The entire section.

Client Comments. “See remarks in item #10.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The audit report clearly states that this is a Navy identification badge, and does not imply that it is a CAC. The congressional response dated October 16, 2006, does clearly state that a CAC cannot be issued without a photo, but it makes no mention of a religious accommodation in another way or of waiving the requirement to receive a CAC.

USD(I) Comments on the Findings

The Director of Security responded for the USD (I). Below are excerpts from the draft report, comments from the USD (I), and audit responses.

Item 1 (page 4, “Automated Verification of Status”)

Excerpt: “DMDC is working . . . to establish an automated capability to verify the status of an individual’s background check.”

Client Comments. “Concur. As part of the E-GOV initiatives, the Department is participating in an E-clearance working group to automate and expedite submission of SF85P electronically, and is working to find an automated capability so that the issuing official is able to verify the status of the individual’s background check at time of PIV issuance.”

Audit Response. We have reviewed client comments and determined report revisions were not required.

Item 2 (page 11, “Background Checks”)

Excerpt: “However, the guidance does not address a vetting process for foreign nationals requiring a CAC...in countries where no international security agreement has been established, such as Afghanistan and Iraq.”

Client Comments. “Concur. The Department is working to define an acceptable vetting process for foreign nationals requiring a CAC in countries where no international security agreement has been established.”

Audit Response. We have reviewed client comments and determined report revisions were not required.

Item 3 (page 5, Note to table showing DoD Employees and Contractors With Incomplete Background Checks)

Client Comments. “Nonconcur with DMDC’s assertion that the data in JPAS is not accurate. We would like to know basis for this assertion.”

Audit Response. In its “Update Homeland Security Presidential Directive (HSPD)-12 Implementation Plan,” January 24, 2008, DMDC included a “Special Note” on numbers of background investigations required. The special note reads as follows:

In an effort to improve the fidelity of the Department’s background investigation numbers, DoD and OPM have begun an initiative to analyze and reconcile over 1 million background investigation records. These numbers may not be an accurate reflection of the completed qualifying investigations and be more a reflection of the DoD JPAS data quality received from the Military Services and Defense Agencies.

Item 4 (page 11, “Background Checks”)

Excerpt: “DoD Components have not met NACI background check requirements.”

Client Comments. “Partially Concur. The Department mandated the National Agency Check with Law and Credit (NACLC) as the minimum investigation for newly accessed service members; on 1 Oct 2005, the Army implemented this mandate for its military accessions. As a result, a large group of earlier accessions have had the Entrance National Agency Check (ENTNAC) conducted. Our initial assessment indicates that conducting a NACI on all the individuals who had previously had the ENTNAC conducted would place a great financial burden on the Army. In order to make fiscally sound decisions, the Department supports the Army request for waiver from the immediate HSPD-12-mandated NACI background checks until members’ current CAC cards expire or individuals are due for periodic investigations. In the meantime, the Department has been working to validate the number that does not meet the NACI background check requirements. DMDC is continuing to check their database against OPM records, as some of the individuals have had investigations conducted which are not included in their database. Some individuals have had the NACLC conducted, which the Department considers equivalent to the NACI. Considering the above, when the assessment has been completed, the number who has not met NACI background check requirements will be significantly less than initially projected and the Department can then prioritize submission of NACI’s on the remainder.”

Audit Response. We reviewed client comments and determined that report revisions were not required. DMDC has reported that multiple Defense Components have noncompliant investigation records. Any DoD Component requesting a waiver of HSPD-12 NACI requirements should formally document the request and notify OMB.

Item 5 (page 13, “NACI Requirement”)

Excerpt: “DoD Regulation 5200.08-R . . . leaves open such questions as which DoD entity should pay for the background checks for contractors, and what kind of background check is required for foreign nationals.”

Client Comments. “Regarding payment for background checks for contractors: There are clearly defined procedures governing how investigations are to be submitted to OPM, and how these are billed and financed. Each service is responsible for submitting and paying for investigations conducted on their contractors. (Note: This is separate and distinct from investigations required for contractors requiring classified access. Such investigations are submitted in accordance with the provisions of the National Industrial Security Program, and are programmed for and funded by the Defense Security Service.)”

Audit Response. We reviewed client comments and determined that report revisions were not required. Guidance for non-Federal employees (contractors or vendors) who require only routine physical access to DoD installations and who may not previously have been subject to a background investigation should be included in the HSPD-12

implementation guidance. It should be made clear that DoD Components are to follow existing guidance when appropriate for each category of non-Federal employees.

Item 6

Client Comment. “Insert other appropriate references for physical security, physical security equipment and access control authorities.

- DoDD 5143.01, Under Secretary of Defense for Intelligence (USD(I)), Nov 23, 2005
- DoDI 5200.8, Security of DoD Installations and Resources, Dec 10, 2005
- DoDI 3224.3, Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E), Oct 1, 2007
- DoDD 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the DoD, Jan 7, 1980 (policy being transferred/incorporated from DoD IG to USD(I)
- DoDD 5000.1, The Defense Acquisition System, May 12, 2003
- OSD 12922-05, DoD Policy for Biometric Information for Access to U.S. Installations and Facilities in Iraq, Jul 15, 2005.”

Audit Response. The requested references appear in the bulleted list above.

ASD NII/CIO Comments on the Findings

The Deputy Assistant Secretary of Defense, Information and Identity Assurance responded for the ASD(NII)/CIO. His itemized comments and our audit responses appear below.

Item 2[†] (page 2, “Background”)

Client Comments. “The following three statements in this paragraph are inaccurate: 1) ‘Agencies may elect to implement HSPD-12 through either a transitional³ or an end-point credential’. ‘Transitional’ and ‘end-point’ refer to PIV card interfaces and are not mentioned in FIPS 201-1 or OMB 05-24. 2) ‘DoD must achieve the end-point credential specification for all cardholders at some point’. This statement is inferred from SP 800-73-1 and is not mentioned in the normative sections of the FIPS 201 standard. 3) ‘OMB has established October 27, 2006 as the date for issuing an initial end-point credential by all nontransitional agencies; however, ...’ According to OMB 05-24, all agencies begin compliance with FIPS 201, Part 2 as of October 27, 2006. Issuing PIV cards with the end-point card interface is not a stated requirement in the normative sections of FIPS 201. There is no milestone date published (in FIPS 201 or SP 800-73) for ‘Legacy’ PKIs to issue PIV cards with the end-point interface. Recommend rewriting the paragraph to accurately state the PIV card issuance and implementation requirements as listed in FIPS 201, Part 1 & 2, and the implementation milestones published in the OMB memo 05-24.”

Audit Response. We reviewed client comments and determined that report revisions were not required. As stated in FIPS 201-1, the interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in NIST Special Publication 800-73, “Interfaces for Personal Identity Verification,” March 2006. NIST SP 800-73 states that a FIPS 201-1 PIV-II card specification is described in Part 3 of SP 800-73, and all agencies must ultimately comply with Part 3 in accordance with the schedule provided by OMB in its Memorandum M-05-24.

Item 3

Client Comments. “The definition of ‘credential’ specified in the glossary of the report is inaccurate and unreferenced. It is unclear to the reader of the report why a definition of ‘credential’ is needed in the report at this time. If a definition of credential is needed, recommend the definition in NIST’s SP 800-63-3 ‘Electronic Authentication Guidelines’ is used. Recommend removing the footnote and the definition from the glossary.”

[†] Item 1 refers to a recommendation, rather than to the finding.

Audit Response. We reviewed client comments and determined that report revisions were not required. See FIPS 201-1, Appendix F – Glossary of Terms, Acronyms, and Notations, for the definition of “credential.”

Item 4

Client Comments. “The definition of ‘interoperability’ specified in the glossary of the report is incomplete and unreferenced. It is unclear to the reader of the report why a definition of ‘interoperability’ is needed in the report at this time. The PIV card will be interoperable with Federal government physical or logical access control systems based on compliance with the FIPS standard. Recommend removing the footnote and the definition from the glossary.”

Audit Response. We reviewed client comments and determined that report revisions were not required. See FIPS 201-1, Appendix F – Glossary of Terms, Acronyms, and Notations, and NIST 800-73-1, Section 1.3, for the definition of “interoperability.”

Item 5 (page 3, first paragraph 1)

Client Comments. “This paragraph is inaccurate and confusing. The impression left with the reader is that DoD has failed to accomplish any of the PIV Part 1 or PIV Part 2 requirements. The term ‘strategic pause’ is not defined or explained, yet is listed as the reason for missing critical milestones. The term ‘HSPD-12 minimum standards’ is used but it is not clear what minimum standards are being referenced. The word ‘transitional’ is used however there is no definition or context to provide the reader with an understanding of its meaning. HSPD-12 is a federal directive to develop and implement a standard identity credential. The phrase ‘DoD has not met HSPD-12 minimum standards for its transitional program’ has no relevance to implementing required Agency actions in Atch A, para 2b of OMB 05-24. From the paragraph, the reader is led to assume that there is a requirement for agency’s to centrally fund HSPD-12 implementation. There is not such requirement in HSPD-12 or the OMB-05-24. Recommend rewriting the paragraph and conclusions based on supportable evidence. For example: DoD has not been able to fully comply with the Agency actions (milestones) involving background investigation, as identified in Atch A, para 3B of OMB 5-24. Failure to fully complete these actions could delay obtaining the full benefit of having HSPD-12/FIPS 201 compliant credentials issued to all eligible DoD recipients.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The January 2008 update of the DoD HSPD-12 Implementation Plan states that in April 2007 DoD instituted a strategic pause. The strategic pause directly affected DoD’s ability to support HSPD-12. FIPS 201-1, parts I and II, establishes “HSPD-12 minimum standards.” OMB required all agencies to begin issuing compliant credentials by October 27, 2006, either through the services of GSA and the Department of Interior or by performing this function internally. DoD’s internal transitional program was not exempt from this requirement. DoD transitional status does allow DoD additional time to obtain full operational capability because of the large volume of

compliant credentials to be issued. In the report glossary, Appendix D, we have included the definition of “transitional.” The report does not state that centralized funding is required. However, we requested that USD(I) and USD(P&R) consider implementing central funding.

Item 6 (page 3, paragraph 3)

Client Comments. “The fact that DMDC had to declare a ‘strategic pause’ indicates that there was a plan to transition the existing DoD CAC issuance infrastructure to a FIPS 201 compliant configuration within the mandated timeframe. The report discounts any credit for attempting to comply with FIPS 201 or for informing OMB of DoD’s progress toward the milestones and the challenges that DOD encountered. In the discussion of the ‘strategic pause’ in this paragraph, recommend a fuller investigation of the reasons for the ‘strategic pause.’ Given that there was an original plan that assumedly would have accomplished OMB milestones, the reasons for declaring a pause would be illustrative to DoD leadership, especially if further investigation could identify occurrences of flaws in planning, ineffective internal management, funding challenges or the indications of lack of leadership buy-in or oversight.”

Audit Response. We reviewed client comments and determined that report revisions were not required. Our report discusses the impact of the strategic pause on implementing HSPD-12 milestones, and we did not review the reasons for instituting the strategic pause.

Item 7 (page 4, “Automated Verification of Status”)

Client Comments. “The statement ‘... DoD does not intend to produce identity credentials that will include an electronic indication...’ is misleading and unsubstantiated. It is apparently taken from a September 2006 update in the [JANDODPLAN]. Further investigation of the most current plans for issuing the DoD’s PIV credential would uncover that the investigation status of the DoD PIV card recipient will be electronically distinguishable to systems interfacing with the card. The final sentence in the paragraph leads the reader to believe that DoD has not and never intended to comply with this FIPS 201 Part II requirement. The discussion of Auto Verification Status in this paragraph appears to be quite limited and does not give any indication of the enormity of the task required to make IT systems from disparate Federal Agencies (i.e. DoD, DSS, OPM, FBI) electronically communicate, the cost, time and manpower it takes to initiate required investigations of employees or “CAC eligible” contractors or the lead time and development risks involved with restructuring the CAC issuance infrastructure. Establishing an electronic mechanism to check the investigation status of a credential recipient at the time of credential issuance, in real time, continues to be a formidable challenge and one that is continuing to be pursued. Recommend this paragraph be removed from the report.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The updated January 2008 DoD HSPD-12 Implementation Plan did not update the status of the NACI indicator, and we were not provided with information to the contrary.

Item 8 (page 4, “Deadlines for Completion of Background Checks”)

Client Comments. “This paragraph gives no indication about how the failure to comply with the stated OMB milestones impacts either the effectiveness of DoD’s HSPD-12 implementation, the quality and security of the PIV credential or DoD employee’s ability to interoperate with physical access or logical IT systems. The impression left with the reader is that DoD has failed to accomplish this requirement and that has left DoD with a worthless and non-functional credential. Recommend this paragraph is rewritten to provide some ‘leadership relevant’ information. A discussion of the immediate and longer term impacts of the failure to initiate appropriate background investigations needs to be included in this paragraph. For instance, Can the milestone failure be viewed as a ‘symptom’ of the Department’s lack of strong centralized management or funding of the HSPD-12 mandate?, poor coordination between DoD organizations?, or lack of DoD leadership emphasis at the highest levels?”

Audit Response. We reviewed client comments and determined that report revisions were not required. We reported that DoD did not meet the OMB deadline of October 27, 2007, for background checks for employees and contractors employed for less than 15 years. DoD should assess the impact and take the necessary management steps to comply with HSPD-12.

Item 9 (page 5, “Privacy Requirements”)

Client Comments. “The Privacy Requirements (PrivRqmts) section of the report makes no mention of any of the privacy related requirements mentioned in OMB memo 05-24 or FIPS 201. Neither does the report identify the extent to which the DoD’s implementation has accomplished compliance with HSPD-12 privacy requirements. While it may be in the purview of the DODIG to mention other privacy related issues involving the content or topology of the HSPD-12 credential, to have only discussion of the findings and shortcomings of the DoD SSN reduction effort in the PrivRqmts section of the HSPD-12 report is confusing to the reader and does not provide a clear tie between DoD’s Geneva Convention Identification Card, the Common Access Card or DoD’s PIV-compliant credential. The applicability and impacts of SSN reduction on the HSPD-12 requirement is left to the reader to figure out. The finding stated in the 2nd to last sentence of paragraph 10, ‘The current appearance of DoD’s Geneva Convention credential unnecessarily compromises....,’ is an unsubstantiated and unsupported assertion and should be removed from the report. This statment is inappropriate for this report without an investigation of what are the topographical requirements for a Geneva Conventions Card and why is DoD’s Geneva Conventions card currently produced with this information. Recommend separating the discussion and findings regarding the DoD SSN reduction effort into a separate section of this report with a descriptive section heading

that is distinct from a HSPD-12/PIV privacy discussion. Recommend the SSN reduction section include specific discussion that identifies the relationship between the DoD Geneva Convention Identification Card, the DoD CAC and DoD's PIV compliant credential and why the advance of technology has created vulnerabilities by exposing the SSN and other PII on identification credentials."

Audit Response. We reviewed client comments and determined that report revisions were not required. The USD(P&R) is taking the necessary actions to address privacy concerns with the next-generation PIV-related Geneva Conventions credential. For additional information, see USD(P&R) comments, Appendix C, Item #5.

Item 10 (page 6, "DoD PIV PKI Authentication Certificate")

Client Comments. "The PKI PMO decided to develop a fourth DoD PKI certificate to meet PIV requirements because modifying existing DoD PKI certificates presented unacceptable operational impacts to the DoD PKI. As a legacy PKI (defined in section 5.4.4 of FIPS 201), DoD has lobbied aggressively and gained NIST's acceptance of proposed FIPS 201 changes that would allow legacy PKIs to continue to assert Legacy PKI policy OIDs [object identifiers]. Alternative acceptable OIDs will not materially affect the the security characteristics or interoperable use of the PIV issued PKI certificates and provides legacy PKIs, such as DoD, with much needed clarity on the implementation of the PIV standard. However, NIST has not as yet made the change to FIPS 201 for unrelated reasons. DoD's inability and unwillingness to make adjustments to the DoD PKI Certificate Policy to align with the Federal Common Policy are based on specific, unacceptable impacts to DoD missions and operations. In an effort to compromise and be able to become fully PIV compliant with the FIPS in the future, DoD requested two changes to the Federal Common Policy. The Federal PKI Policy Authority has acknowledged the rationale for and accepted the changes in principle, but has not as yet voted on the requested changes. A vote must come from the full Federal PKI Policy Authority. This issue is now out of the control of DoD. The 2nd to last sentence in paragraph 14 is a misquote from the [JANDODPLAN] (page 11). This misquoted sentence, 'DoD plans to use common policy object identifiers in the PIV PKI authentication certificate only one year after FIPS is revised to meet DoD objections', comes from the Sept 2006 update regarding the optional Digital Signature certificate, not the PIV Authentication. In the misquoted sentence the word 'only' is inserted giving the reader the impression that DoD intends to assert the FedCommon Policy OIDs for a single year. All actions and decisions made by DoD regarding compliance with the FIPS requirements for the PIV Auth [authentication] certificate have been within its purview and with the intention of becoming fully PIV compliant at some point in the future. With this in mind, recommend these paragraphs are rewritten to include a discussion of DoD PKI efforts regarding the PIV Auth certificate requirement and a review and consideration of the justification for those efforts as stated in the [JANDODPLAN]."

Audit Response. We reviewed client comments and determined that report revisions were not required. We reported that proposed changes have been submitted to the

Federal PKI Policy Authority for approval but that no date has been established for consideration of the two modifications. Further, we have received no indication that the changes will be promulgated in policy. We did not use the phrase “for only 1 year.” We used “only 1 year” to emphasize that DoD will not assert Common Policy object identifiers until 1 year after FIPS 201-1 or Common Policy is modified.

Item 11 (page 11, “DoD Component Implementation Efforts”)

Client Comments. “The 1st sentence in the paragraph, ‘HSPD-12 requires that access to Federal facilities or information systems be granted only to Federal employees and contractors with secure and reliable credentials.’, does not accurately paraphrase direction stated in either HSPD-12 or OMB 05-24 regarding use of standard identity credentials to access facilities or information systems. In HSPD-12 and OMB 05-24, direction states that personnel (both government employees and eligible contractors) will use the standard credential for physical and logical access to Federal resources. These references, however, do not restrict access to Federal facilities or Federal Information systems to only holders of a PIV-compliant credential. Recommend rewriting the paragraph to restate the HSPD-12 and OMB direction more accurately.”

Audit Response. We reviewed client comments and have edited “HSPD-12 requires that access to Federal facilities or information systems be granted only to Federal employees and contractors with secure and reliable credentials.” The sentence now reads: “HSPD-12 requires that access to Federal facilities or information systems be granted to Federal employees and contractors based on secure and reliable forms of identification that meet the Federal standard established by the Secretary of Commerce.”

Item 12 (page 11, “DoD Component Implementation Efforts and Background Checks”)

Client Comments. “The 2nd sentence in paragraph 3 is inaccurate and misleading. A more accurate phrasing of the issue would be to say that the percent of completion of the task (OMB 05-24, Atchmt A, para 3.B) to initiate the NACI background investigations for current DoD civilian employees, military members and eligible contractors varies between the Components. In the first sentence of paragraph 4, it has to be assumed by the reader that the report is again referring to the same OMB 05-24 task. Lack of accurate references called out in the report make it difficult to understand the relevance and meaning of statements in the report. Recommend rewriting the report to include relevant references to all HSPD-12, FIPS 201 or OMB established requirements. These requirements are the basis for determining DoD’s compliance or consistency and should be clearly identified.”

Audit Response. We reviewed client comments and determined that report revisions were not required. The second sentence of paragraph 3 on page 11 is accurate and not misleading. OMB Memorandum M-05-24, Attachment A, Table 2B, states that by October 27, 2007, agencies are to verify and/or complete required background

investigations for all current employees and contractors employed less than 15 years. DoD failed to meet the requirement.

Item 13 (page 12, “DBIDS Credentials”)

Client Comments. “The finding in this paragraph is unsubstantiated and inaccurate. Empirical or anecdotal evidence is not provided to corroborate the finding. Issuance of a physical access only credential to contractor personnel with a routine requirement for only physical access to facilities is allowed under the OMB 05-24, Atchmt A, para 1.C. DBIDS cards should not have been issued to DoD employees in lieu of the CAC. If this did happen, it should have been noted as a procedural error and corrected as soon as noted. Recommend removing this paragraph from the report.”

Audit Response. We reviewed client comments and determined that report revisions were not required. We disagree that issuance of a physical-access-only credential to contractor personnel with a routine requirement for only physical access to facilities is allowed under OMB Memorandum M-05-24, Attachment A, paragraph 1.C. This paragraph states that HSPD-12 applies to “individuals under contract to a department or agency requiring routine access to federally controlled facilities and/or federally controlled information systems to whom you would issue Federal agency identity credentials, consistent with your existing security policies” and “does not apply to individuals under contract to a department or agency, requiring only intermittent access to federally controlled facilities.”

Item 14 (page 13, “DBIDS Credential and Physical Access Control System”)

Client Comments. “This paragraph misrepresents the referenced direction from DoD Regulation 5200.08-R. From how this paragraph is worded, the reader is led to believe that 5200.08-R directs that all DoD employees and contractors authorized routine physical access to a single installation should be issued a DBIDS card in lieu of a CAC. While it is conceded that para C.3..3.2 in DoD 5200.08-R applies to personnel with only single installation access requirements and there may be DoD employees that only need access to a single federal facility to perform their job, it should recognized that DoD 5200-08-R does not override the requirement to issue a CAC to all DoD employees. Recommend removing this paragraph from the report.”

Audit Response. We reviewed client comments and determined that report revisions were not required. DoD Regulation 5200.08-R states that the DBIDS card shall be issued and authorized for routine, physical access to a single DoD installation or facility. The Regulation does not specify the category of employees or contractors to receive the DBIDS card. OUSD(I) has agreed to remove paragraph C3.3.2. in its entirety.

Item 15 (page 13, “DBIDS Credential and Physical Access Control System”)

Client Comments. “The DBIDS access control system and the accompanying DBIDS credential was never intended to be a PIV compliant credential and therefore should not have comply with the full gamut of PIV Part I or II requirements. To a lesser assurance

level than asserted by the CAC or a PIV-compliant credential, the DBIDS credential, due to its registration and issuance process, can adequately verify the claimed identity of individuals seeking access to facilities. Even though it was developed prior to FIPS 201, the DBIDS credential issuance incorporates elements of two of the four PIV Part I control objectives, (i.e. rapidly authenticated electronically and issued by accredited and authoritative credential providers). Recommend removing these paragraphs from the report.”

Audit Response. We reviewed client comments and determined that report revisions were not required. USD(I) has responsibility for DoD physical access control policy and has stated that DoD Regulation 5200.08-R will be revised to require all electronic access control systems to meet HSPD-12 and OMB guidance.

Item 16 (page 14, “Photo Identification Requirements”)

Client Comments. “The discussion in these paragraphs has more to do with a lack of Department internal controls over credentialing processes than compliance with OMB 05-24, HSPD-12 or FIPS 201. The situation, as described is regrettable and does point out the interrelated nature of credentialing, access control and proofing and vetting of personnel. Recommend separating the discussion regarding issuance of a photoless ID prior to HSPD-12 into a separate section of this report. The section should also inform DoD leadership of the critical need to synchronize identity related activities across the Department under an Identity Management Principal Staff Assistant.”

Audit Response. We reviewed client comments and determined that report revisions were not required. We agree that DoD leadership should be informed of the critical need to coordinate identity-related activities across the Department.

Appendix D. Glossary

1) *Access Control* - The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

2) *Certificate Revocation List* - A list of revoked public key certificates created and digitally signed by a certification authority.

3) *Credential* - Evidence attesting to one's right to credit or authority; in this standard, it is the PIV card and data elements associated with an individual that authoritatively bind an identity (and, optionally, additional attributes) to that individual.

4) *Common Policy* - Policy framework governing the Public Key Infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates six specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices, a high-assurance user policy, a user authentication policy, and a card authentication policy.

5) *End-point* - Status granted to agencies without a smart card program; has all the elements required for PIV compliance.

6) *Federal Bridge Certification Authority* - Consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among principal entity certification authorities.

7) *Interoperability* - allows any Government facility or information system, regardless of the PIV issuer, to verify a cardholder's identity using the credentials on the PIV card; the use of PIV identity credentials such that client-application programs, compliant card applications, and compliant integrated circuit cards can be issued interchangeably by all information-processing systems across Federal agencies.

8) *National Agency Check (NAC)* - The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index, Defense Clearance and Investigation Index, FBI Name Check, and FBI National Criminal History Fingerprint Check.

9) *National Agency Check with Inquiries (NACI)* - The basic and minimum investigation required on all new Federal employees; consists of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past 5 years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes employment, 5 years; education, 5 years and highest degree verified; residence, 3 years; references; law enforcement, 5 years; and NACs.

10) *NextUpdate* - Time required by the Common Policy to update the Certificate Revocation List.

11) *Object Identifiers* - A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, object identifiers are used to uniquely identify certificate policies and cryptographic algorithms.

12) *PIV end-point applet* - program that will allow the end-point scanners and readers to read and retrieve end-point information from the DoD PIV credential. This is DoD's solution to comply with HSPD-12 interoperability requirements.

13) *PIV authentication certificate* - shall be an asymmetric private key supporting card authentication for an interoperable environment; is mandatory for each PIV Card.

14) *Public Key Infrastructure (PKI)* - A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

15) *Transitional* - Status granted to agencies with smart card programs as an intermediate step; transitional credential is not end-point compliant.

Appendix E. List of Acronyms and Abbreviations

ASD(NII)/CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
ASD	Assistant Secretary of Defense
AOR	Area of Responsibility
CAC	Common Access Card
CIOs	Chief Information Officers
CI&S	Counterintelligence and Security
CONUS	Continental United States
CRL	Certificate Revocation List
DASD(IIA)	Deputy Assistant Secretary of Defense (Information and Identity Assurance)
DBIDS	Defense Biometrics Identification System
DHRA	Defense Human Resource Agency
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DLAI	Defense Logistics Agency Instruction
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoD IG	Department of Defense Inspector General
DSCP	Defense Supply Center Philadelphia
DSS	Defense Security Service
DTM	Directive Type Memorandum
E-GOV	Electronic Government
ENTNAC	Entrance National Agency Check
EUCOM	European Command
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FPCON	Force Protection Condition
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive-12
ID	Identification
IOC	Initial Operational Capability
IT	Information Technology
JANDODPLAN	January 2008 DoD Implementation Plan
JPAS	Joint Personnel Adjudication System
JTF-GNO	Joint Task Force Global Network Integration
NAC	National Agency Check

NACI	National Agency Check with Written Inquiries
NACLC	National Agency Check with Law and Credit
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	Naval Support Activity
OCONUS	Outside Continental United States
OIDs	Object Identifiers
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OUSD(P&R)	Office of the Under Secretary of Defense for Personnel and Readiness
PACs	Physical Access Controls
PACOM	Pacific Command
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMO	Program Management Office
PSAs	Principal Staff Assistants
RAPIDS	Real-time Automated Personnel Identification System
RSA	Rivest, Shamir, and Adleman
SSN	Social Security Number
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

Under Secretary of Defense for Personnel and Readiness Comments



PERSONNEL AND
READINESS

OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

APR 17 2008



MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Comments on Draft Report on DoD Implementation of Homeland Security
Presidential Directive-12 (Project No. D2007-D000LB-0153.000)

Thank you for the opportunity to review and provide comments on the draft report
"DoD Implementation of Homeland Security Presidential Directive-12," Project No. D2007-
D000LB-0153.000, dated March 21, 2008.

We note that some recommendations provided for our office do not fall under the
Office of the Under Secretary for Personnel and Readiness (OUSD (P&R)) area of
responsibility. Additionally, in some instances, the draft report goes beyond the scope of
Homeland Security Presidential Directive-12 (HSPD-12), associated National Institute of
Science and Technology (NIST) publications, or relevant Office of Management and Budget
(OMB) guidance memorandums on HSPD-12.

Our responses to the draft report recommendations are included in Attachment 1. We
have also provided comments on 19 excerpts from the report that we believe are not
completely accurate or do not fall within the scope of HSPD-12. These comments are
included in Attachment 2 for your review. Please feel free to direct any questions to Mr.
Francis Jones (703.696.0179, francis.jones@osd.pentagon.mil) or Ms. Heidi Boyd
(703.696.0404, heidi.boyd@osd.pentagon.mil).

Jeanne B. Fites
Deputy Under Secretary of Defense
(Program Integration)

Attachments:
As stated:

cc:
Under Secretary of Defense for Intelligence
Assistant Secretary of Defense for Networks and Information Integration / DoD Chief
Information Officer



**Attachment 1: Office of the Secretary of Defense For Personnel and Readiness
(OUSD P&R) Comment to DoD IG Draft Report “DoD
Implementation of HSPD-12” (Project # D2007-D000LB-0153.00)**

Recommendations Requiring OUSD (P&R) Comment - Findings A:

1. “We recommend that the Under Secretary of Defense for Personnel and Readiness:
 - a. Submit DoD’s proposed personal identity verification end-point credential to the General Services Administration for conformance testing and approval within 1 month of completion of recommendation A.3.
 - b. Test the General Services Administration-approved personal identity verification credential for compatibility with DoD systems before making it available to DoD employees and contractors.
 - c. Implement the recommendation in DoD’s Report to Congress, “Omission of the SSN from the Department of Defense Military Identification Cards,” May 23, 2007, to display only the last four digits of the Social Security number on the Geneva Convention credential within 2 months, while migrating toward completely eliminating the display of the Social Security number on all identification credentials.”
2. “We recommend that the Under Secretary of Defense for Personnel and Readiness, in conjunction with the Under Secretary of Defense for Intelligence, centrally fund the acquisition and installation of HSPD-12-compliant access control equipment throughout the Department and establish Component-specific milestones for both acquisition and installation of the equipment.”

OUSD (P&R) Response to Recommendations in Findings A:

- 1.a. OUSD (P&R) concurs with this recommendation. OUSD (P&R) will submit its Common Access Card (CAC) Personal Identity Verification (PIV) end-state credential to the General Services Administration (GSA) for conformance/interoperability testing within one month of completion of recommendation A3 (expected by the end of 2008). OUSD (P&R) fully expects the card to pass all areas DoD has agreed to support in accordance with the January 2008 DoD HPSD-12 Implementation Plan.
- 1.b. OUSD (P&R) partially concurs with this recommendation. As outlined in the above response, DoD will conduct GSA conformance testing by the end of calendar year 2008. However, OUSD (P&R) non-concurs with completing GSA testing before making the credential available to DoD employees and contractors. DoD was approved by OMB as a legacy card issuer and, as such, is authorized to implement transitional credentials that can be updated in the future to conform to FIPS 201 specifications. This provides significant benefit with minimal adverse impact to the operational community. Additionally, DoD has an established testing process with the Military Services and DoD Components that is monitored by the DoD’s Identity Protection Senior Coordinating Group (IPMSCG). Prior to being moved to our operational CAC

inventory, all emerging CAC platforms (including DoD's CAC PIV transitional and end-state configurations) are evaluated and approved for release by the IPMSCG's Test and Evaluation Work Group (TEWG). This group consists of representatives from Military Service CAC-PKI labs and several DoD Components.

1.c. OUSD (P&R) partially concurs with this recommendation. We note that the implementation of DoD's Report to Congress, "Omission of the SSN from the Department of Defense Military Identification Cards," May 23, 2007 is not a requirement of HSPD-12, associated NIST standards, or relevant OMB HSPD-12 guidance.

The Department is executing the policy, procedural and technical steps required to remove the SSN from DoD ID cards. The truncation of the visible SSN on Geneva Conventions credential to four-digits is one step in the plan recommended to Congress. However, this step will take place in a coordinated fashion as the feature is made available within the issuance software (e.g., RAPIDS) and existing credentials are replaced after the update is completed. We expect to begin implementing this change during calendar year 2008.

2. OUSD (P&R) defers on a response to this recommendation; the responsibility for centrally funding the acquisition and installation of access control equipment does not fall under the purview of OUSD (P&R). Responsibility for force protection and physical security standards falls under the purview of the Office of the Under Secretary of Defense for Intelligence (OUSD (I)).

Recommendations Requiring OUSD (P&R) Comment – Findings B:

1. "We recommend that the Under Secretary of Defense for Personnel and Readiness develop and coordinate comprehensive milestones for full compliance with HSPD-12 requirements within 3 months.
2. We recommend that the Under Secretary of Defense for Personnel and Readiness, in conjunction with the Under Secretary of Defense for Intelligence, within 3 months:
 - a. Revise DoD Directive 1000.25 to incorporate the FIPS 201-1 minimum requirements in all DoD electronic access control systems used to identify personnel requiring routine access to DoD installations.
 - b. Develop minimum background check requirements for vetting foreign nationals where no international security agreement exists, such as Iraq and Afghanistan.

OUSD (P&R) Response to Recommendations in Findings B:

1. OUSD (P&R) concurs with this recommendation. DoD is working from the January 2008 DoD HSPD-12 Implementation Plan which outlines the Department's milestones for meeting those Federal conformance and interoperability capabilities we have agreed to support. However, OUSD (P&R) recognizes the need to coordinate additional milestones for areas that fall under the purview of other OSD PSAs (i.e., personnel security / background vetting). OUSD

P&R will work with these organizations within the next three months to identify milestones that can be incorporated into the DoD HSPD-12 Implementation Plan.

2.a. OUSD (P&R) defers on a response to this recommendation; the responsibility for incorporating the minimum requirements for electronic access control systems does not fall under the purview of OUSD (P&R). OUSD (I) is the DoD lead for Physical Security to include the standards for access control. OUSD (P&R) will cooperate fully to support OUSD (I) with the development of these requirements and recommends that any subsequent guidance be incorporated within force protection or physical security publications or issuances such as the DoD Regulation 5200.8R issued by OUSD (I).

2.b. OUSD (P&R) defers on a response to this recommendation; the responsibility for personnel security standards does not fall under the purview of OUSD (P&R). OUSD (I) is the DoD lead for Personnel Security to include the standards for equivalent HSPD-12 vetting for Foreign Nationals. OUSD (P&R) will fully cooperate with OUSD (I) on incorporating identified requirements into the card issuance process and associated guidance.

OUSD (P&R) Additional Comments on Recommendations - Findings B:

OUSD (P&R) offers additional comments on the following recommendation provided to OUSD (I):

B.3.b. "We recommend that the Under Secretary of Defense for Intelligence suspend use of the Defense Biometric Identification System and any other alternative credentials not explicitly approved by the Under Secretary of Defense for Intelligence for physical access to DoD installations and facilities."

OUSD (P&R) non-concurs with the recommendation to suspend the use of the Defense Biometric Identification System (DBIDS). This access control system is installed throughout Europe, Korea, Japan, Guam, the AOR (except Iraq and Afghanistan) and some locations in CONUS, for a total of 157 bases. The use of this system has substantially increased security at each of the bases where it is used compared to the historical use of "flash and pass" processes. To suspend usage of this system would significantly degrade security at each of these bases where it is currently operating or defer improvement in security at those bases where DBIDS implementations are planned. OUSD (P&R) would concur with a recommendation that DBIDS migrate to meet the policy published by OUSD (I).

**Attachment 2: Clarification of Statements within DoD IG Draft Report
"DoD Implementation of HSPD-12" (Project # D2007-D000LB-0153.00)**

Item #1 (page 2, Section "Background")

Excerpt: *"As of March 2007, DoD has issued 56 such credentials;"*

CLARIFICATION: As outlined in our March 2008 PIV issuance report to OMB, DoD has issued 108,778 PIV transitional configured CACs.

page 1

Item #2 (page 2, "Internal Controls")

Excerpt: "Implementing the recommendations made in this report, *together with those developed for a related audit, Project No. D2007-D000LA-0199, "Controls Over the Contractor Common Access Card Life Cycle,"* will assist in bringing the Department into compliance. A copy of the final report will be provided to the senior official responsible for internal controls in DoD."

CLARIFICATION: It is inappropriate to reference an incomplete audit which draft results have not been shared with organizations engaged with the audit. DoD IG recommendations and findings related to Project No. D2007-D000LA-0199 should be addressed by a separate audit through the formal audit review processes.

Item #3 (page 3, Section "DoD Implementation of HSPD-12")

Excerpt: *"DoD failed to meet the milestones approved by the Office of Management and Budget (OMB) in 2005 for compliance with HSPD-12 by 2010"*

CLARIFICATION: DoD has updated its original HSPD-12 Implementation Plan to OMB on two occasions (most recently 24 January 2008). OMB approved our initial revision (September 2006) and is currently reviewing our January 2008 revision.

Item #4 (page 5, "Deadlines for Completion of Background Checks")

Excerpt: "According to DoD's January 2008 implementation plan, as of December 26, 2007, that the following *number of DoD employees and contractors have not completed the required background checks:* Military/Civilian (1,240,214); contractors (196,185); total (1,436,399)."

CLARIFICATION: The numbers provided within the DoD's January 2008 Implementation Plan reflected efforts taken to reconcile CAC issuance records with JPAS. The 1,436,399 number are records that showed as "unknown" during this effort, but does not mean that these individuals do not have background investigations. The use of the term "have not completed" is not accurate.

page 4

Item #5 (page 5, "Privacy Requirements")

Excerpt: *"DoD Geneva Conventions credential for members of the uniformed service does not comply with HSPD-12 and Federal policies and requirements to reduce identity fraud and protect personal privacy."*

CLARIFICATION: The DoD Geneva Conventions CAC does comply with standards issued for HSPD-12 (see FIPS 201-1 Section 4.1.4.4, pg 20).

"For Zones 9 and 10, departments and agencies are encouraged to use this area prudently and minimize printed text to that which is absolutely necessary.

In the case of the Department of Defense, the back of the card will have a distinct appearance. This is necessary to display information required by Geneva Accord and to facilitate medical entitlements that are legislatively mandated."

The additional references in the "Privacy Requirements" section regarding Social Security Numbers (SSN) are not specifically related to HSPD-12, associated NIST publications, and relevant OMB memoranda (M05-24) on HSPD-12. In fact, the Administration's initiative to reduce the use and exposure of SSN within the Federal Government began in April 2007 with the release of the Presidential Task Force on Identity Theft's strategic plan (and subsequent OMB memo M07-16 22 May 2007). Until FIPS 201-1 is updated to align with new Federal policies related to SSNs, this topic is outside the scope of the audit announcement.

DoD has been engaged in the effort to decrease the possibility of our Service members exposure to identity fraud/theft through the Department's use of SSN. USD (P&R) provided a Report to Congress that outlines the Department's plan. We have been working to secure consensus with others within the Department and adjust the necessary paperwork to make sure our proposal satisfies the Geneva Conventions requirements. A directive-type memorandum, "DoD Social Security Number Reduction Plan," was signed by USD (P&R) 29 March 2008.

Item #6 (page 5, "Privacy Requirements")

Excerpt: "No time table was provided to implement the recommendation, however *nor did the report specify who was responsible for implementation*"

CLARIFICATION: Identification cards to support Geneva Conventions and benefits/eligibility are clearly the responsibilities of the USD (P&R). Authorship of the report to Congress, "Omission of the SSN from the Department of Defense Military Identification Cards," May 23, 2007, was led by the OUSD (P&R) and signed by USD (P&R).

Item #7 (page 6, "Personal Identity Verification-II Requirements")

Excerpt: "*DoD did not meet the March 2006 PIV II initial operating capability implementation milestone approved by OMB in the DoD implementation plan, nor did DoD meet the October 2006 OMB milestone for final PIV II implementation.*"

CLARIFICATION: The reference for the March 2006 PIV II IOC date is unclear. The approved DoD HSPD-12 Implementation plan states the following:

- DoD achieved "initial operational capability (IOC) for PIV I" by October 27, 2005
- DoD achieved "IOC for PIV II" with issuance of DoD PIV transitional cards by October 27, 2006

Item #8 (page 8, "DoD Transitional Status")

Excerpt: "...workstations to RAPIDS version 7.2 to produce DoD PIV credentials for DoD CONUS installation by December 12, 2008. *No schedule for deployment of updated RAPIDS workstations has been announced for four OCONUS installations, to include two in Germany and one each in Djibouti and Greenland.*"

CLARIFICATION: The RAPIDS upgrade schedule to produce DoD PIV credentials for calendar year 2008 includes all OCONUS installations in Europe, Africa, and Asia, including those referenced in the excerpt. The only workstations that it does not include are those portable

deployable shipboard and forward deployed units. OUSD (P&R) is working directly with the Services to upgrade these workstations as they return from theater or deployment or have a period of availability.

Item #9 (page 11, “DoD Component Implementation Efforts”)

Excerpts: “...Components have been authorized to issue *Defense Biometric Identification System (DBIDS) credentials instead of PIV credentials*”

CLARIFICATION: DBIDS is a local or regional perimeter access control system that uses the CAC (for those individuals who qualify) and contains local physical access only badging capabilities (for those who do not qualify for a CAC). DBIDS credentials are not issued to those who possess CACs. As such, HSPD-12, associated NIST publications, and relevant OMB memoranda (especially M05-24) on HSPD-12 have nothing to do with DBIDS. This topic is outside the scope of the audit announcement, “DoD Implementation of Homeland Security Presidential Directive-12.”

page 15

Item #10 (page 12, “Photoless Identification”)

Excerpts: “The Department of the Navy Commanding Officer at the Naval Support Station (now Naval Support Activity) in Philadelphia, PA *issued a waiver for a photo identification to a Defense Logistics Agency (DLA) employee working at Defense Supply Center-Philadelphia (DSCP) who objected for religious reasons to having his photograph taken and displayed on the identification badge.*”

CLARIFICATION: The badge in questions is not a CAC. It was a locally issued badge to facilitate access to the installation. A congressional response dated October 16, 2006 stated that a special exemption to policy could not be approved through OUSD (P&R), to receive a CAC without a picture, but if the religion could be accommodated in another way, then OUSD (P&R) could waive the requirement to receive a CAC. This is the only documented request across 3.5 million active CACs.

page 16

Item #11 (page 12, Authorized DBIDS Credentials”)

Excerpts: “...authorized *Components to issue a DBIDS card to employees and contractors that require routine physical access only. This deviates from established HSPD-12 policy.*”

CLARIFICATION: DBIDS cards are not issued to DoD civilian or military personnel—those individuals receive CACs. Identification of those contractors who are to receive a PIV card is based on the Department’s determination of the access requirement. DoD has defined eligible CAC contractors in the following manner in the draft “Next Generation CAC Implementation Guidance” directive-type memorandum (DTM), signed into the SD 106 staffing process on 6 March 2008:

page 16

“CAC eligibility for other populations, including DoD contractors, non-DoD Federal civilians, state employees, and other non-DoD affiliates, is based on the government sponsor’s determination of the type and frequency of access required to DoD facilities or networks that will effectively support the mission. To be eligible for a CAC, the access requirement must meet one of the following criteria:

- The individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of DoD (this requirement is applicable to DoD contractors only).

- The individual requires both access to a DoD facility and access to DoD networks on site or remotely.
- The individual requires remote access to DoD networks that use only the CAC logon for user authentication.”

Item #12 (page 12, “DoD HSPD-12 Policy and Guidance”)

Excerpt: “...established a working group to develop comprehensive guidance for implementation of HSPD-12 but the group *has made limited progress during its existence*”

CLARIFICATION: The HSPD-12 workgroup has made significant progress since its inception. A Deputy Secretary of Defense level Directive Type Memorandum (DTM) on HSPD-12 policy is in formal SD106 coordination. In addition, an SD 106 coordination request was signed by Dr. Chu for a DTM on the “Next Generation CAC Implementation Guidance” on 5 March 2008. Additionally, several sub-working groups have been established and are meeting to directly address issues regarding personnel security and vetting criteria in compliance with HSPD-12, and to set standards for access control to DoD installations and facilities.

page 16

Item #13 (page 12, “DoD HSPD-12 Policy and Guidance”)

Excerpt: “*Meanwhile, DoD senior management chose to establish and implement less stringent access control requirements than those established by HSPD-12*”

CLARIFICATION: HSPD-12, associated NIST publications, and relevant OMB guidance do not provide specific mandates or timetable for the use of HSPD-12 credentials to control access to Federal network assets or installations. In fact, the CAC was implemented in 2000 and has provided a secure and reliable identification card prior to the release of HSPD-12 so that it is used daily to:

- Facilitate access to DoD facilities and installations around the world.
- Authenticate to 98% of the Department’s unclassified network accounts and 100% of the Departments private web servers, web sites, and portals. This has resulted in:
 - Successful intrusions declining **46 percent** in the past year because of a requirement that all DOD personnel log on to unclassified networks using CACs, although there are 6 million probes of Defense Department networks a day. (JTF GNO, Lt. Gen. Charles Croom, Federal Computer Weekly article on 25 January 2007)
 - The Number of successful socially engineered e-mail attacks (*definition: A socially engineered attack is one in which the user is somehow tricked into doing the attacker’s bidding*) against DoD users – a practice known as spear phishing – declining **30 percent** in the past year (JTF GNO, Lt. Gen. Charles Croom, Federal Computer Weekly article on 25 January 2007)

page 16

Item #14 (page 13, “Issuance of Guidance”)

Excerpt: “DoD Regulation 5200.8-R ... *is inconsistent with HSPD-12 because it allows DBIDS and other forms of identification that are not compliant with FIPS 201-I*”

CLARIFICATION: See remarks in item #16.

page 17

Item #15 (page 13, “DBIDS Credential and Physical Access Control System”)

Excerpt: “OMB instructed agencies to be careful not to develop policies that contradict HSPD-12 standards for identity proofing and issuance of credentials. HSPD-12 standards mandate that all Federal employees and contractors requiring routine access for 180 days or greater receive a

page 17

PIV-compliant credential and under a NACI or equivalent background check. DoD Regulation 5200.8-R authorizes personnel requiring only routine physical access to receive a DBIDS credential and undergo the less rigorous NAC. ***Granting routine access to DoD installations to personnel who have only a NAC background check does not fully comply with the HSPD-12 policy objective to enhance security and protect physical and human capital assets on DoD installations.***

CLARIFICATION: See remarks in item #16.

Item #16 (page 13, “DBIDS Credential and Physical Access Control System”)

Excerpt: “Yet the system does not meet the minimum standards of FIPS 201-1 to verify the claimed identity of individuals seeking physical access to Federal Government facilities...DBIDS uses card readers and scanners that are not on the Approved Products List as required by OMB”

CLARIFICATION: DBIDS is a local or regional perimeter access control system that uses the CAC (for those individuals who qualify) and contains local physical access only badging capabilities (for those who do not qualify for a CAC). DBIDS credentials are not issued to those who possess CACs. As such, HSPD-12, associated NIST publications, and relevant OMB memo on HSPD-12 have nothing to do with DBIDS. This topic is outside the scope of the audit announcement, “DoD Implementation of Homeland Security Presidential Directive-12.”

Item #17 (page 13, “DBIDS Credential and Physical Access Control System”)

Excerpt: “Neither, the DBIDS system nor the card, are configured to operate with HSPD-12 required security features such as, the PKI certificates, CHUID, and biometric embedded in the ICC of the credential”

CLARIFICATION: See remarks in item #18.

Item #18 (page 13, “DBIDS Credential and Physical Access Control Systems”)

Excerpt: “Further, the use of barcode technology on the DBIDS credential does not enhance security due to the inability of the barcode (static physical card feature) to deter fraud, counterfeiting, and protect privacy ... DBIDS does not meet the FIPS 201-1 minimum standards to enhance security, increase government efficiency, and protect personal privacy”

CLARIFICATION: See remarks in item #13. Additionally, individuals who receive local access badges or DBIDS credentials typically do not receive CACs (e.g., DoD PIV credential). There is no place within HSPD-12, FIPS 201 or OMB M05-24 that specifies access control rules/criteria for physical installations and/or IT assets covering personnel who do not qualify for CACs or Federal PIVs. The type of background investigations conducted on these individuals is outside the scope of HSPD-12.

Moreover, PKI is not intended to be used in the physical access control environment. DBIDS, which predates HSPD-12, is a complementary not competing system. DBIDS:

- Went operational on 9/11/2001 in Korea
- Was built to optimize interoperability through use of bar code technologies
- Managed risk by using local or regionally stored biometrics for authentication which minimizes risk of fake/fraudulent cards
- Is scalable to FPCON levels
- Is able to provide information sharing across a region

page 17

page 17

pages 17, 18

Item #19 (page 14, “Photo Identification Requirements”)

Excerpt: The entire section.

CLARIFICATION: See remarks in item #10.

pages 18, 19

Under Secretary of Defense for Intelligence Comments



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000


MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Comments on Draft Report on DoD Implementation of Homeland Security
Presidential Directive-12 (Project No. D2007-D000LB-0153.000)

We have received the draft report "DoD Implementation of Homeland Security Presidential Directive (HSPD)-12," dated March 12, 2008 and appreciate the opportunity to comment. Our response is attached.

After review, we note that some recommendations do not fall within the purview of the Office of the Under Secretary of Defense for Intelligence, we therefore address who should be consulted in our comments.

My point of contact is Mrs. Donna Rivera at (703) 604-1172, or donna.rivera@osd.mil.


Gregory Torres
Director of Security

Attachments:
As stated

cc:
Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Policy
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense for Network and Information Integration/ DoD Chief
Information Officer



**Attachment 1: Office of the Under Secretary of Defense for Intelligence (OUSD (I))
Comment to DoD IG Draft Report “DoD Implementation of HSPD-12” (Project #
D2007-D000LB-0153.00)**

Recommendations Requiring OUSD (I) Comment – Findings A2:

A.2 We recommend that the Under Secretary of Defense for Personnel and Readiness, in conjunction with the Under Secretary of Defense for Intelligence, centrally fund the acquisition and installation of HSPD-12-compliant access control equipment throughout the Department and establish Component-specific milestones for both acquisition and installation of the equipment.

OUSD (I) nonconcurs with the recommendation as currently stated. OUSD (P&R) has the responsibility for fielding a FIPS 201 compliant identification credential to Federal Employees and Contractors only, which is expected to be complete by the end of FY 2012. OUSD (P&R) does not have Research, Development, Test and Evaluation (RDT&E), acquisition or oversight authority for access control equipment.

We do not support a central acquisition approach for access control equipment at present, as we are not staffed to support oversight of an effort of this magnitude, nor is the Air Force, who is the lead for Research, Development, Test and Evaluation for access control physical security equipment. See references DoDI 5143.01, Under Secretary of Defense for Intelligence (USD (I)), Nov 2, 2005 and DoDI 3224.3 Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E), Oct 1, 2007.)

Central acquisition will be problematic for all components, as there are other issues that would significantly impact this approach. These issues include: Congress provided no funding to implement this mandate and therefore any centralized acquisition would require reductions in other Physical Security and Department procurement requirements; HSPD-12 does not apply to National Security Systems and Special Risk Security Provisions; ability to adapt existing legacy systems to meet HSPD12; and the install of access control equipment must be in concert with military design and construction projects for access control points.

OUSD (I) concurs that any new acquisition and installation of access control equipment throughout the Department must conform to the mandates of HSPD-12 and associated OMB policy for interoperability. This stipulation has been included in formally staffed draft policy, Directive Type Memorandum 08-004, Policy Guidance for DoD Access Control, which is pending USD (I) signature as of this submission.

Recommendations Requiring OUSD (I) Comment – Findings B:

B.2. We recommend that the Under Secretary of Defense for Personnel and Readiness, in conjunction with the Under Secretary of Defense for Intelligence, within 3 months:

B.2.a. Revise DoD Directive 1000.25 to incorporate the FIPS 201-1 minimum requirements in all DoD electronic access control systems used to identify personnel requiring routine access to DoD installations.

OUSD (I) nonconcurs. P&R is not the Principal Staff Assistant for Security, Access Control or Physical Security Equipment, which includes electronic access control systems. DoDD 1000.25 must be revised to delete all references to same. DoDI 5200.8 and DoDD 5200.8R will be revised to require all electronic access control systems to meet HSPD 12 and OMB guidance. OUSD(I) will coordinate with OSD (AT&L) to exercise RDT&E of all procurements for electronic access control systems in coordination with the Components physical security representatives and electronic systems engineers. OUSD(I) will maintain oversight IAW DoDI 5143.01.

B.2.b. "Develop minimum background check requirements for vetting foreign nationals where no international security agreement exists, such as Iraq and Afghanistan.

OUSD (I) concurs. The Department (CI&S), in conjunction with the Federal Interagency Working Group and with USD (Policy), ASD (International Security Affairs) is working to define an acceptable vetting process for foreign nationals requiring a CAC or physical access only badge in countries where no international security agreement has been established.

B.3 We recommend that the Under Secretary of Defense for Intelligence:

B.3.a.(1) Require all contractors and Federal employees requiring routine physical access to a DoD installation to undergo a NACI background investigation and receive a DoD PIV credential"

OUSD (I) concurs.

B.3.a (2) Expressly prohibit the issuance and use of photoless identification credentials used to gain access to DoD installations and facilities, or establish a formal process to waive requirements for a photo on the credential.

OUSD (I) concurs in part. OSD (P&R) is the proponent for CAC and Identification Card issuance. OUSD (I) is the proponent for physical access only credentials and will issue guidance to incorporate requirements mandated by Section 1069 of the 2008 National Defense Authorization Act. OUSD (I) will incorporate in policy procedures that "unescorted" access will not be granted for persons who do not present a photo identification credential. The federally compliant PIV credential and any physical access only credential will be required to be displayed as a visual access badge. Reasonable accommodation may be made for persons without photo identification, which will include "escorted" access, if an escort is available.

B.3.a (3) Delete paragraph C.3.3.2 in its entirety and delete reference to the Defense Biometric Identification System credential in paragraph C.3.3.3 of the Installation Access section.

OUSD (I) concurs. OUSD (I) has incorporated this stipulation in formally staffed draft policy, Directive Type Memorandum 08-004, Policy Guidance for DoD Access Control, which is pending USD (I) signature as of this submission and has added language that all upgrades or procurement of access control systems be FIPS 201 compliant.

B.3.b Suspend use of the Defense Biometric Identification System (DBIDS) and any other alternative credentials not explicitly approved by the Under Secretary of Defense for Intelligence for physical access to DoD installations and facilities.

OUSD (I) concurs in part. OUSD (I) will not suspend use of existing legacy access control systems, which includes DBIDS until such time as we have identified, tested and certified a replacement or upgrade that meets FIPS 201, Security Equipment Integration and network security requirements. Suspending use of existing legacy access control systems, whether FIPS compliant or not, would degrade the only security mitigators we have in place at the present time. The Directive Type Memorandum 08-004, Policy Guidance for DoD Access Control will require Heads of DoD components when purchasing upgrades to existing access control systems or when replacing current systems, the upgraded system must meet FIPS 201 (including ISO 14443 contactless technology and ability to perform automated personal identity verification); include an emergency power source; and have the ability to provide rapid electronic authentication to Federal and DoD authoritative databases, including DoD personnel registered in the Defense Enrollment and Eligibility Reporting System. This change in policy will prohibit the procurement of non FIPS 201 compliant systems.

**Attachment 2: Office of the Under Secretary of Defense for Intelligence (OUSD (I))
Comment to DoD IG Draft Report “DoD Implementation of HSPD-12” (Project #
D2007-D000LB-0153.00) Comments on text:**

Page 4, “Automated Verification of Status”

DMDC and CI&S... establish an automated capability to verify the status of an individual’s background check:

COMMENT: Concur. As part of the E-GOV initiatives, the Department is participating in an E-clearance working group to automate and expedite submission of SF85P electronically, and is working to find an automated capability so that the issuing official is able to verify the status of the individual’s background check at time of PIV issuance.

Page 4, “Background Checks”

“guidance does not address a vetting process for foreign nationals requiring a CAC... in countries where no international security agreement has been established, such as Afghanistan and Iraq.”

COMMENT: Concur. The Department is working to define an acceptable vetting process for foreign nationals requiring a CAC in countries where no international security agreement has been established.

Page 5, “Subscript to DoD Employees and Contractors With Incomplete Background Checks”

COMMENT: Nonconcur with DMDC’s assertion that the data in JPAS is not accurate. We would like to know basis for this assertion.

Page 11, “Background Checks”

DoD Components have not met NACI background check requirements.

COMMENT: Partially Concur.

The Department mandated the National Agency Check with Law and Credit (NACLC) as the minimum investigation for newly accessed service members; on 1 Oct 2005, the Army implemented this mandate for its military accessions. As a result, a large group of earlier accessions have had the Entrance National Agency Check (ENTNAC) conducted. Our initial assessment indicates that conducting a NACI on all the individuals who had previously had the ENTNAC conducted would place a great financial burden on the Army. In order to make fiscally sound decisions, the Department supports the Army request for waiver from the immediate HSPD-12-mandated NACI background checks until members’ current CAC cards expire or individuals are due for periodic investigations. In the meantime, the Department has been working to validate the number that does not meet the NACI background check requirements. DMDC is continuing to check their database against OPM records, as some of the individuals have had investigations conducted which are not included in their database. Some individuals

page 15

have had the NACLIC conducted, which the Department considers equivalent to the NACI. Considering the above, when the assessment has been completed, the number who has not met NACI background check requirements will be significantly less than initially projected and the Department can then prioritize submission of NACI's on the remainder.

Page 13. "NACI Requirement"

"which DoD entity should pay for the background checks for contractors, and what kind of background check is required for foreign nationals."

Regarding payment for background checks for contractors:

There are clearly defined procedures governing how investigations are to be submitted to OPM, and how these are billed and financed. Each service is responsible for submitting and paying for investigations conducted on their contractors. (Note: This is separate and distinct from investigations required for contractors requiring classified access. Such investigations are submitted in accordance with the provisions of the National Industrial Security Program, and are programmed for and funded by the Defense Security Service.)

General comment:

Insert other appropriate references for physical security, physical security equipment and access control authorities.

- DoDD 5143.01, Under Secretary of Defense for Intelligence (USD (I)), Nov 23, 2005
- DoDI 5200.8, Security of DoD Installations and Resources, Dec 10, 2005
- DoDI 3224.3, Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E), Oct 1, 2007
- DoDD 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the DoD, Jan 7, 1980 (policy being transferred/incorporated from DoD IG to USD (I))
- DoDD 5000.1, The Defense Acquisition System, May 12, 2003
- OSD 12922-05, DoD Policy for Biometric Information for Access to U.S. Installations and Facilities in Iraq, Jul 15, 2005

page 17

Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Comments



NETWORKS AND
INFORMATION
INTEGRATION

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MAY 15 2008

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Draft DODIG Report "DoD Implementation of Homeland Security
Presidential Directive-12, Project No. D2007-D000LB-0 153.000"

Thank you for the opportunity to review this draft DODIG report. Our comments are provided in the attachment.

In general, the report's tone and implications raise many concerns. It does not present a fair and balanced view of the Department's efforts, failing to acknowledge the enormous amount of work done to fully implement the HSPD-12 mandate. Request a meeting to discuss these concerns at your earliest convenience.

Our points of contact for this matter are Mr. Morris Hymes, mahyme1@missi.ncsc.mil, (410) 854-4900, and Mr. Don Fuller, Donald.Fuller.ctr@osd.mil, (703) 604-0500.

Robert F. Lentz
Deputy Assistant Secretary of Defense
(Information and Identity Assurance)

Attachment:
As stated



Attachment 1: DASD IIA Comments and Recommendations on DoD IG Draft Report
“DoD Implementation of HSPD-12” (Project # D2007-D000LB-0153.00)

Item # 1 (page 9, Recommendations Section, para A.3.)

Excerpt: *A.3. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer develop the mandatory public key infrastructure authentication certificate that complies with FIPS 201-1 requirements to use common policy object identifiers for cross-agency verification of cardholders' identification within 6 months.*

Recommendation: Recommend that the DODIG remove the recommendation A.3 from the final report based on the extenuating and mitigating circumstances surrounding this FIPS 201 requirement. DoD PKI PMO has endeavored, in good faith, to comply with all FIPS 201 requirements. Current plans, as stated in the January 2008 update to the DoD HSPD-12 Implementation Plan [JANDODPLAN], indicate that the PIV_Auth certificate will be instantiated on the DoD PIV credential as soon as technically possible. Lack of compliance with the Common Policy OIDs does not affect the interoperable use (cross-agency verification of cardholder's identity) of the CAC with either DoD or other Federal Agency physical or logical systems.

Comment: Disagree with this recommendation A.3. The recommendation does not recognize or consider the extensive mitigating or extenuating circumstances explained in the January 2008 update to DoD HSPD-12 Implementation Plan [JANDODPLAN] nor does it show consideration of the reported work accomplished by the DoD PKI PMO to comply with the FIPS 201 requirement for instantiation of a PIV Authentication certificate (PIV_AUTH). The DoD PKI PMO has planned for the deployment and is testing the issuance of a PIV_AUTH certificate and has estimated beginning the issuance of this certificate on the DoD PIV credential in 3QFY08 [JANDODPLAN]. Those plans are aligned with but contingent on fielding of another version of the RAPIDS issuance software. The DODIG recommendation does not consider the lack of adequate memory available on the current CAC crypto module, the availability of the cryptomodules with the necessary storage capacity, necessity for performance testing on issuance and use or examination of the operational impacts of using RSA 2048 end entity certificates. The DODIG recommendation does not consider that the DoD PKI PMO has reported, for several years, to OMB and the Federal PKI Policy Authority (FPMI PA), the risks of changing DoD PKI CA operations to conform with the specified Federal Common Policy requirements. DoD PKI PMO has been endeavoring to work with the FPMI PA to make mutually acceptable changes to the Federal Common Policy Certificate Policy (CP). The DODIG recommendation does not recognize or consider in extenuation that the DoD PKI PMO has been very proactive about informing the FPMI PA and NIST about the operational challenges full compliance with FIPS 201 represents to DoD.

Item # 2 (page 2, Background, para 3)

Recommendation: Rewrite the paragraph to accurately state the PIV card issuance and implementation requirements as listed in FIPS 201, Part 1 & 2. and the implementation milestones published in the OMB memo 05-24.

Attachment 1: DASD IIA Comments and Recommendations on DoD IG Draft Report
"DoD Implementation of HSPD-12" (Project # D2007-D000LB-0153.00)

Comment: The following three statements in this paragraph are inaccurate: 1) "*Agencies may elect to implement HSPD-12 through either a transitional³ or an end-point⁴ credential*". "Transitional" and "end-point" refer to PIV card interfaces and are not mentioned in FIPS 201 or OMB 05-24. 2) "*DoD must achieve the end-point credential specification for all cardholders at some point*". This statement is inferred from SP 800-73-1 and is not mentioned in the normative sections of the FIPS 201 standard. 3) "*OMB has established October 27, 2006 as the date for issuing an initial end-point credential by all nontransitional agencies; however, ...*" According to OMB 05-24, all agencies begin compliance with FIPS 201, Part 2 as of October 27, 2006. Issuing PIV cards with the end-point card interface is not a stated requirement in the normative sections of FIPS 201. There is no milestone date published (in FIPS 201 or SP 800-73) for "Legacy" PKIs to issue PIV cards with the end-point interface.

Item # 3 (page 1, Footnote #1)

Recommendation: If a definition of "credential" is needed, recommend the definition in NIST's SP 800-63-3 "Electronic Authentication Guidelines" is used. Recommend removing the footnote and the definition from the glossary.

Comment: The definition of "credential" specified in the glossary of the report is inaccurate and unreferenced. It is unclear to the reader of the report why a definition of "credential" is needed in the report at this time.

Item # 4 (page 2, Footnote #2)

Recommendation: Recommend removing the footnote and the definition from the glossary.

Comment: The definition of "interoperability" specified in the glossary of the report is incomplete and unreferenced. It is unclear to the reader of the report why a definition of "interoperability" is needed in the report at this time. The PIV card will be interoperable with Federal government physical or logical access control systems based on compliance with the FIPS standard.

Item # 5 (page 3, Section A, para 1)

Recommendation: Recommend rewriting the entire paragraph and conclusions based on supportable evidence. For example, the first sentence could read as follows: DoD has not been able to fully comply with the Agency actions (milestones) involving background investigation, as identified in Attachment A, para 3B of OMB 5-24. Failure to fully complete these actions could delay obtaining the full benefit of having HSPD-12/FIPS 201 compliant credentials issued to all eligible DoD recipients.

Comment: This paragraph is inaccurate and confusing. The impression left with the reader is that DoD has failed to accomplish any of the PIV Part 1 or PIV Part 2 requirements. The term "strategic pause" is not defined or explained, yet is listed as the reason for missing critical milestones. The term "HSPD-12 minimum standards" is used but it is not clear what minimum standards are being referenced. The word "transitional" is used however there is no definition or context to provide the reader with an

Attachment 1: DASD IIA Comments and Recommendations on DoD IG Draft Report
"DoD Implementation of HSPD-12" (Project # D2007-D000LB-0153.00)

understanding of its meaning. HSPD-12 is a federal directive to develop and implement a standard identity credential. The phrase "DoD has not met HSPD-12 minimum standards for its transitional program" has no relevance to implementing required Agency actions in Attachment A, para 2b of OMB 05-24. From the paragraph, the reader is led to assume that there is a requirement for agency's to centrally fund HSPD-12 implementation. There is not such requirement in HSPD-12 or the OMB-05-24. The concluding sentence in this paragraph is based on incomplete or inaccurate statements.

Item # 6 (page 3, Section A, para 3)

Recommendation: In the discussion of the "strategic pause" in this paragraph, recommend a fuller investigation of the reasons for the "strategic pause". Given that there was an original plan that assumedly would have accomplished OMB milestones, the reasons for declaring a pause would be illustrative to DoD leadership, especially if further investigation could identify occurrences of deficiencies in planning, ineffective internal management, funding challenges or the indications of lack of leadership buy-in or oversight.

Comment: The fact that DMDC had to declare a "strategic pause" indicates that there was a plan to transition the existing DoD CAC issuance infrastructure to a FIPS 201 compliant configuration within the mandated timeframe. The report discounts any credit for attempting to comply with FIPS 201 or for informing OMB of DoD's progress toward the milestones and the challenges that DoD encountered.

Item # 7 (page 4, Section A, para 6 (Automated Verification of Status))

Recommendation: Recommend this paragraph be removed from the report

Comment: The statement "...DoD does not intend to produce identity credentials that will include an electronic indication..." is misleading and unsubstantiated. It is apparently taken from a September 2006 update in the [JANDODPLAN]. Further investigation of the most current plans for issuing the DoD's PIV credential would uncover that the investigation status of the DoD PIV card recipient will be electronically distinguishable to systems interfacing with the card. The final sentence in the paragraph leads the reader to believe that DoD has not and never intended to comply with this FIPS 201 Part II requirement. The discussion of Automated Verification of Status in this paragraph appears to be quite limited and does not give any indication of the enormity of the task required to make IT systems from disparate Federal Agencies (i.e. DoD, DSS, OPM, FBI) electronically communicate, the cost, time and manpower it takes to initiate required investigations of employees or "CAC eligible" contractors or the lead time and development risks involved with restructuring the CAC issuance infrastructure. Establishing an electronic mechanism to check the investigation status of a credential recipient at the time of credential issuance, in real time, continues to be a formidable challenge and one that is continuing to be pursued.

Item # 8 (page 4, Section A, para 7 (Deadlines for Completion of Background checks))

Recommendation: Recommend this paragraph is rewritten to provide some "leadership relevant" information. A discussion of the immediate and longer term impacts of the

Attachment 1: DASD IIA Comments and Recommendations on DoD IG Draft Report
"DoD Implementation of HSPD-12" (Project # D2007-D000LB-0153.00)

failure to initiate appropriate background investigations needs to be included in this paragraph. For instance, Can the milestone failure be viewed as a "symptom" of the Department's lack of strong centralized management or funding of the HSPD-12 mandate? , poor coordination between DoD organizations? , or lack of DoD leadership emphasis at the highest levels?

Comment: This paragraph gives no indication about how the failure to comply with the stated OMB milestones impacts either the effectiveness of DoD's HSPD-12 implementation, the quality and security of the PIV credential or DoD employee's ability to interoperate with physical access or logical IT systems. The impression left with the reader is that DoD has failed to accomplish this requirement and that has left DoD with a worthless and non-functional credential.

Item # 9 (page 5, Section A, para's 8-10 (Privacy Requirements))

Recommendation: Recommend separating the discussion and findings regarding the DoD SSN reduction effort into a separate section of this report. That section should be distinct from a HSPD-12/PIV privacy discussion. Recommend the SSN reduction section include specific discussion that identifies the relationship between the DoD Geneva Convention Identification Card, the DoD CAC and DoD's PIV compliant credential and why the advance of technology has created vulnerabilities by exposing the SSN and other PII on identification credentials.

Comment: The Privacy Requirements (PrivRqmts) section of the report makes no mention of any of the privacy related requirements mentioned in OMB memo 05-24 or FIPS 201. Neither does the report identify the extent to which the DoD's implementation has accomplished compliance with HSPD-12 privacy requirements. While it may be in the purview of the DODIG to mention other privacy related issues involving the content or topology of the HSPD-12 credential, to have only discussion of the findings and shortcomings of the DoD SSN reduction effort in the PrivRqmts section of the HSPD-12 report is confusing to the reader and does not provide a clear tie between DoD's Geneva Convention Identification Card, the Common Access Card or DoD's PIV-compliant credential. The applicability and impacts of SSN reduction on the HSPD-12 requirement is left to the reader to figure out. The finding stated in the 2nd to last sentence of paragraph 10, "*The current appearance of DoD's Geneva Convention credential unnecessarily compromises...*", is an unsubstantiated and unsupported assertion and should be removed from the report. This statement is inappropriate for this report without an investigation of what are the topographical requirements for a Geneva Conventions Card and why is DoD's Geneva Conventions card currently produced with this information.

Item # 10 (page 6, Section A, para 12-14 (DoD PIV PKI Authentication Certificate))

Recommendation: All actions and decisions made by DoD regarding compliance with the FIPS requirements for the PIV Auth certificate have been within its purview and with the intention of becoming fully PIV compliant at some point in the future. With this in mind, recommend these paragraphs are rewritten to include a discussion of DoD PKI efforts

Attachment 1: DASD IIA Comments and Recommendations on DoD IG Draft Report
"DoD Implementation of HSPD-12" (Project # D2007-D000LB-0153.00)

regarding the PIV Auth certificate requirement and a review and consideration of the justification for those efforts as stated in the [JANDODPLAN].

Comment: The PKI PMO decided to develop a fourth DoD PKI certificate to meet PIV requirements because modifying existing DoD PKI certificates presented unacceptable operational impacts to the DoD PKI. As a legacy PKI (defined in section 5.4.4 of FIPS 201), DoD has lobbied aggressively and gained NIST's acceptance of proposed FIPS 201 changes that would allow legacy PKIs to continue to assert Legacy PKI policy OIDs. Alternative acceptable OIDs will not materially affect the security characteristics or interoperable use of the PIV issued PKI certificates and provides legacy PKIs, such as DoD, with much needed clarity on the implementation of the PIV standard. However, NIST has not as yet made the change to FIPS 201 for unrelated reasons. DoD's inability and unwillingness to make adjustments to the DoD PKI Certificate Policy to align with the Federal Common Policy are based on specific, unacceptable impacts to DoD missions and operations. In an effort to compromise and be able to become fully PIV compliant with the FIPS in the future, DoD requested two changes to the Federal Common Policy. The Federal PKI Policy Authority has acknowledged the rationale for and accepted the changes in principle, but has not as yet voted on the requested changes. A vote must come from the full Federal PKI Policy Authority. This issue is now out of the control of DoD. The 2nd to last sentence in paragraph 14 is a misquote from the [JANDODPLAN, page 11]. This misquoted sentence, "*DoD plans to use common policy object identifiers in the PIV PKI authentication certificate only one year after FIPS is revised to meet DoD objections*", comes from the Sept 2006 update regarding the optional Digital Signature certificate, not the PIV Authentication. In the misquoted sentence the word "only" is inserted giving the reader the impression that DoD intends to assert the FedCommon Policy OIDs for a single year.

Item # 11 (page 11, Section B, para 2 (DoD Component Implementation Efforts).)
Recommendation: Recommend rewriting the paragraph to restate the HSPD-12 and OMB direction more accurately.

page 15

Comment: The 1st sentence in the paragraph, "*HSPD-12 requires that access to Federal facilities or information systems be granted only to Federal employees and contractors with secure and reliable credentials.*", does not accurately paraphrase direction stated in either HSPD-12 or OMB 05-24 regarding use of standard identity credentials to access facilities or information systems. In HSPD-12 and OMB 05-24, direction states that personnel (both government employees and eligible contractors) will use the standard credential for physical and logical access to Federal resources. These references, however, do not restrict access to Federal facilities or Federal information systems to only holders of a PIV-compliant credential.

Item # 12 (page 11, Section B, para 3 and 4 (DoD Component Implementation Efforts and Background checks))
Recommendation: Recommend rewriting the report to include relevant references to all HSPD-12, FIPS 201 or OMB established requirements. These requirements are the basis for determining DoD's compliance or consistency and should be clearly identified.

page 15

Attachment 1: DASD IIA Comments and Recommendations on DoD IG Draft Report
“DoD Implementation of HSPD-12” (Project # D2007-D000LB-0153.00)

Comment: The 2nd sentence in paragraph 3 is inaccurate and misleading. A more accurate phrasing of the issue would be to say that the percent of completion of the task (OMB 05-24, Attachment A, para 3.B) to initiate the NACI background investigations for current DoD civilian employees, military members and eligible contractors varies between the Components. In the first sentence of paragraph 4, it has to be assumed by the reader that the report is again referring to the same OMB 05-24 task. Lack of accurate references called out in the report make it difficult to understand the relevance and meaning of statements in the report.

Item # 13 (page 12, Section B, para 7 (DBIDS Credentials).)

Recommendation: Recommend removing this paragraph from the report.

page 16

Comment: The finding in this paragraph is unsubstantiated and inaccurate. Empirical or anecdotal evidence is not provided to corroborate the finding. Issuance of a physical access only credential to contractor personnel with a routine requirement for only physical access to facilities is allowed under the OMB 05-24, Attachment A, para 1.C. DBIDS cards should not have been issued to DoD employees in lieu of the CAC. If this did happen, it should have been noted as a procedural error and corrected as soon as noted.

Item # 14 (page 13, Section B, para 13 (DBIDS Credential and Physical Access Control System))

Recommendation: Recommend removing this paragraph from the report.

page 17

Comment: This paragraph misrepresents the referenced direction from DoD Regulation 5200.08-R. From how this paragraph is worded, the reader is led to believe that 5200.08-R directs that all DoD employees and contractors authorized routine physical access to a single installation should be issued a DBIDS card in lieu of a CAC. While it is conceded that para C.3.3.2 in DoD 5200.08-R applies to personnel with only single installation access requirements and there may be DoD employees that only need access to a single federal facility to perform their job, it should be recognized that DoD 5200-08-R does not override the requirement to issue a CAC to all DoD employees.

Item # 15 (page 13, Section B, para's 14-15 (DBIDS Credential and Physical Access Control System))

Recommendation: Recommend removing these paragraphs from the report.

pages 17, 18

Comment: The DBIDS access control system and the accompanying DBIDS credential was never intended to be a PIV compliant credential and therefore should not have comply with the full gamut of PIV Part I or II requirements. To a lesser assurance level than asserted by the CAC or a PIV-compliant credential, the DBIDS credential, due to its registration and issuance process, can adequately verify the claimed identity of individuals seeking access to facilities. Even though it was developed prior to FIPS 201, the DBIDS credential issuance incorporates elements of two of the four PIV Part I control

Attachment 1: DASD IIA Comments and Recommendations on DoD IG Draft Report
“DoD Implementation of HSPD-12” (Project # D2007-D000LB-0153.00)

objectives: a DBIDS card can be rapidly authenticated electronically and is issued by a accredited and authoritative credential provider

Item # 16 (page 14, Section B, para's 18-20 (Photo Identification Requirements))
Recommendation: Recommend separating the discussion regarding issuance of a photoless ID prior to HSPD-12 into a separate section of this report. That section should also inform DoD leadership of the critical need to synchronize identity related activities across the Department under an Identity Management Principal Staff Assistant.

pages 18,19

Comment: The discussion in these paragraphs has more to do with a lack of Department internal controls over credentialing processes than compliance with OMB 05-24, HSPD-12 or FIPS 201. The situation, as described, is regrettable and does point out the interrelated nature of credentialing, access control and proofing and vetting of personnel.

Item # 17 (page 16, Section B, Recommendations: Recommendation B.3a. (3))
Excerpt: *(3) Delete paragraph C.3.3.2 in its entirety and delete the reference to the Defense Biometric Identification System credential in paragraph C.3.3.3 of the Installation Access section.*

page 22

Recommendation: Recommend removing Recommendation B.3.a. (3) from the report.

Comment: It is documented that the Defense Biometric Identification System (DBIDS) was originally developed to meet a specific physical access credential requirement in EUCOM and PACOM prior to the issuance of HSPD-12. The vetting requirements included in the original DBIDS credential issuance process were specifically suited for populations of people that were not going to be eligible for a PIV-compliant credential. The DBIDS credential provided overseas commanders with a physical access only credential that raised the level of protection afforded to physical facilities while complying with best practices for electronically authenticated credential use.

No where in the text of this report is it acknowledged that the HSPD-12 mandate and FIPS 201 identity credential standard does not apply to populations of personnel, other than employees or contractors, which have a legitimate requirement to access Federal installations or facilities on a routine or intermittent basis. DBIDS can meet the security, proofing, revocation and tracking requirements for populations such as volunteers, maintenance and supply vendors, unpaid interns, employees of non-military concessions and businesses operating within installations or facilities.

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Readiness and Operations Support prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Donald A. Bloomer
Kathryn Truex
Robert R. Johnson
Celia J. Harrigan
Gloria Young
Bradley M. Heller
Giormary Peluyera
LeBarron Durant
Bryan T. Clark
Xavier R. Zayas
Allison E. Tarmann



Inspector General Department *of* Defense